



Prescribing Services

# **DOTTIE**

## **Data Protection by Design**

VERSION DATE

2021-03-24

NOTES

Original Draft

AUTHOR

Emma Cooper, Kafico Ltd

**KAFICO**  
— INFORMATION · GOVERNANCE · CONSULTANCY —



---

## 1. PROJECT CONTEXT

---

DOTTIE is an e-learning platform (DOTTIE: Disease Optimisation Training Through Individualised Education), based on the popular open-source website Moodle (used by most universities as their e-learning platform). Originally it was planned to give training for healthcare professionals (e.g. HCAs) on carrying out certain tasks, such as measuring blood pressure, via videos and PowerPoint presentations, with some assessment functionality (quizzes, a workbook they can submit) to verify they have completed the training. Dottie is a project whereby PSL can offer organisations the ability to upload training materials and their staff login in to complete them. The interface can either integrate with a staff member's already activated NHS Pathways account or they can create a new account. Dottie allows for the employer to review the results of their staff training on a dashboard as well as whether the module is completed.

---

## 2. DATA FLOWS

---

1. Existing PSL customers (GP Practices) will send an email to the PSL Support address to request that PSL activate the DOTTIE training platform for an individual and to enrol them on particular modules.
2. If the user has an NHS Pathways account, the existing data (email address, name) will be used by PSL to create an account on the DOTTIE site. because users would have already used 2-factor authentication to log into NHS Pathways.
3. A password will be generated for them and used to secure their DOTTIE account.
4. This will automatically be entered for them when they navigate from NHS Pathways to DOTTIE via a click of a button (a seamless login experience, without them having to enter the details themselves).
5. The button currently sends via a link to an encrypted page requiring username and password.
6. The login page requires that they enable cookies on their browser.

7. If user does not have an NHS Pathways account, then the request to PSL must include the user's email address and name.
8. Once the DOTTIE account has been created, the new user will be emailed.
9. If they are an existing Pathways user, guidance on accessing the system will be emailed to the address that PSL hold for them. This guidance will explain that access to the system is via a button within their password-protected NHS Pathways interface.
10. If they do not have a Pathways account, a registration confirmation email will be sent to their provided email address. This will contain their login details (email address and a generated password) and the link to access the system directly (<https://dottie.nhspathways.org>).
11. A separate confirmation of DOTTIE user registration will be emailed to the authoriser as per usual process for NHS Pathways user creation. This message will not contain any personal details regarding the user's DOTTIE account.
12. On logging in, materials are available to teach healthcare workers how to use PSL systems, putting more linking in place between the site and NHS pathways (such as buttons next to questionnaires that healthcare workers go over with shielded patients).
13. DOTTIE would not be capturing information about the patient, it would be giving more background to the healthcare worker about a specific question (e.g. for a question on adequate exercise, a link to a training module could give background on what would count as adequate exercise).





## **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 a low 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?	Business Hours Support (8am-6pm) Mon-Fri (not BH). Service Availability 98%. DR optional - dependant on outcome of BIA.
Rationale	System is an enhancement to an existing clinical tool. It allows users of the system to undertake training but the system is currently being used effectively without this addition.
What score has the project been given in terms of the nature and volume of data being processed?	Low volume of personal data involved / high volumes of anonymised data.
Rationale	The system only includes basic demographics of staff as well as the training they have undertaken.
	BRONZE

Overall risk score given to the processing activity / project in question.	
Does the project involve introduction of a cloud service to be assessed?	Introduces cloud services that will need to be assessed
Does the project involve access by data subjects to their own personal data that requires a 'high' level of authentication (i.e. access to their own health or finance records)?	No High Level authentication activities
Does the project involve access by data subjects to their own personal data requiring a 'low' level of authentication (i.e. access to training records)?	Staff access to own training records

---

## 6. RISK ASSESSMENT CONCLUSION

---

The project has been assessed to have an overall risk score of BRONZE 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.”<sup>1</sup>

---

## 2. DATA CONTROLLERS

---

GP Practices has 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.

---

<sup>1</sup> <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.
  - The data subjects are their employees
  - 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
- 

## 2. 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.

AWS 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.

---

### 3. 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.”<sup>2</sup>

Prescribing Services has the following in place;

- A Processing Contract between PSL and GP Practices

---

<sup>2</sup> <https://ico.org.uk/for-organisations/accountability-framework/contracts-and-data-sharing/>



- A Processing Contract between PSL and AWS

---

## ● PROCESSING CONTRACT REVIEW

---

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.

Query – Dottie needs adding to this contract.

**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
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	Yes	2.9.4

international organisation, unless required to do so by law and in those cases will notify the Controller?		
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:** Amazon Web Services

**Contract reviewed:** [AWS 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 5



Does the contract state that the processor shall not engage another processor without prior specific or general written authorisation of the controller?	Yes	Section 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 categories of data subjects and the obligations and rights of the controller?	Yes	Section 1.3
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	
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	Section 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	Section 9
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	Section 14
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	Section 10.3







## 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 \(ICO Guide\)](#)

# 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 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 therefore requires a lawful basis under Art 6 UK GDPR.

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 (1) (f) Legitimate Interests





## 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.  DOTTIE data subjects (employees) are largely already able to access personal data held about them through their account login. However, the system provides an audit trail of access to and changes made within the system 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.



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	Yes, the right to Erasure does apply when processing is for legitimate interests.	The data subjects' ability to have their personal data erased can be facilitated by the system. Any requests will be managed with the oversight of the Controller customer.
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 can be facilitated by the system. Any requests will be managed with the oversight of the Controller customer.
Automated Decision Making	Not Applicable	Not Applicable





**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.



---

## PROPORTIONALITY

---

In accordance with the above risk assessment, the project has been defined as having a **BRONZE** 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.

---

## SECURITY OF DATA IN TRANSIT AND AT REST

### - CLOUD HOSTING AMAZON WEB SERVICES

---

Since the project involves the transfers of data through a network architecture, this assessment has obtained a number of assurances for data in transit between the cloud environment and end users as well as at rest within the cloud environment.

These assurance items are based on the [NHS Digital Health and Social Care Cloud Security – Good Practice Guide](#).

- Queried whether the provider has confirmed that they have taken any steps necessary to ensure that the cryptography offered by AWS (TLS Version 1.2) is in place and active for this project. Such that communications between cloud components are encrypted to recognised best practice standards.
- Queried whether provider has taken steps to ensure that the max encryption levels offered by AWS are active for this project. Such that communications between cloud

data centres are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.

- Queried whether provider has taken steps to ensure that the max encryption levels offered by AWS are active for this project. Such that communications between cloud admin portal and the cloud are encrypted to TLS Version 1.2 or above OR IPsec or TLS VPN gateway as defined by NIST SP800-57.
- AWS architecture utilise strong cryptography as defined by NIST SP800-57 to encrypt communications between the Cloud and the End-user. Confirmed by AWS <https://aws.amazon.com/blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints/>
- Stakeholders to provide more information about the location of hosted data and the safeguards in place for any international transfers
- Query - AWS provides the ability to apply encryption facilities to ensure that no data is written to storage in an unencrypted form. Has the provider ensured that this facility is active for this project.
- Queried whether the provider applies the AWS secure key management services, providing strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1'. The service must provide detailed audit reporting on access of the keys.
- Queried whether the provider confirms that the project utilises the AWS strong cryptography for data at rest as defined by the current version of NIST SP800-57?
- Queried with provider whether the data at rest encryption is tested annually against a recognised standard such as ISO or FIPS 140-2 to test the encryption
- Queried with provider whether their use of AWS key management solutions utilises strong cryptography as defined by the current version of NIST and FIPS standards. e.g. NIST SP800-57 Part 1
- The provider has deployed the application across multiple AWS Availability Zones in the same region for fault tolerance and low latency.
- AWS customers are protected by Amazon's firewall service called Shield as standard.



- AWS has given assertions regarding their data sanitisation approach for cloud storage. If the customer needs a specific standard/method of sanitisation such as DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") the customer can use a secure delete tool which behaves on the AWS storage in the same way it would on a local physical disk.. The provider has confirmed they will delete data on request of the controller and that the appropriate deletion tool will be used in accordance with the risk posed by the data therein.
- Regarding equipment disposal, AWS is certified with ISO/IEC 27001:2013, and CSA STAR CCM v3.0.1.
- AWS security protections and control processes (including sanitisation) are independently validated by multiple third-party independent assessments:  
<https://aws.amazon.com/compliance/programs/>
- "AWS operates our data centers in alignment with the Tier III+ guidelines, but we have chosen not to have a certified Uptime Institute based tiering level so that we have more flexibility to expand and improve performance. AWS' approach to infrastructure performance acknowledges the Uptime Institute's Tiering guidelines and applies them to our global data center infrastructure design to ensure the highest level of performance and availability for our customers."

---

## PHYSICAL SECURITY

---

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

- Data held by PSL 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

---

## 2. 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.

DOTTIE allows employees to access basic personal data such as training records and so for this product, the system permits direct system access for data subjects.

- Queried with stakeholders about whether the system provides the user with a privacy policy which they must actively engage with prior to access
- Queried with stakeholder whether the data subject interface allows 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
- ["Querying with stakeholders which measures are in place to prevent replay attacks"]
- Due to the low risk and low volume personal data being access, authentication is single factor



- Since the authentication is single factor, the data subject is required to enter a username and password
- Queried with stakeholders whether password is at least 8 characters long but does NOT set a maximum length.
- Queries whether the system explains the password constraints to data subjects
- Queried with stakeholders about whether the system prevents commonly used passwords for data subjects
- Queried with stakeholders whether data subject password changes are only required when there has been actual or potential compromise
- Queried whether the system gives data subject users between 5 and 10 attempts to enter their password correctly before locking their account or do any further security checks
- The system hides data subject passwords by default
- The system allows users to paste their password
- Queried whether passwords are stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards
- Queried whether, when the data subject logs in, they are able to see when the credentials were last used
- If a data subject enters their account details incorrectly, the system conceals whether they got the username or password wrong.

---

## SYSTEM AUDIT

---

The project involves the use of 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.
- Queried whether the system / software allows 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.
- Queried whether the system / software satisfies 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.
- Queried with stakeholders whether the audit trail includes 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)
- Queried with stakeholders whether there is 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".
- Queried with stakeholders whether successful login audit data includes User id, date and time (to the second).
- Queried with stakeholders whether unsuccessful login audit data includes Number of attempts, Date and time, Access point (if available), User id (if available)
- Queried with stakeholders whether Password Change audit data includes user id, User whose password was changed, Date and time, end-user device (or Solution) identification information.

---

## 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;

- Queried with stakeholders whether password is at least 8 characters long but does NOT set a maximum length.
- Queried with stakeholder whether, when password is changed, the professional user receive an alert making them aware that their password has recently been changed
- Queried whether the system explains the password constraints to professional users
- Queries with stakeholders about whether the system gives users between 5 and 10 attempts to enter their password correctly before locking their account or do any further security checks
- Queried with stakeholders about whether the system hides passwords by default
- Queried with stakeholders whether the system allows users to paste their password
- Queried with stakeholder whether Passwords are stored salted and hashed, using algorithms and strengths recommended in NIST Cryptography Standards
- Queried with stakeholders about whether, when the professional user logs in, they are able to see when the credentials were last used
- Queried with stakeholders whether if a professional user enters their account details incorrectly, the system conceals whether they got the username or password wrong
- Queried with stakeholder whether, 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
- Queried with stakeholder whether, when password is changed, the professional user receive an alert making them aware that their password has recently been changed
- Queried with stakeholder whether the software allows different privileges for different job roles
- Queried with stakeholder whether the role that they are logged in under presents itself on screen throughout their use of the system
- Queried with stakeholder whether the organisation that they are logged in under present itself throughout their use of the system?

- Queried with stakeholders whether users can have more than one role. For example, they might be Privacy Officer and GP.
- Queried with stakeholders whether the system provides information about the start date, end date and current status (active / inactive) of the roles
- Queried with stakeholders whether the system is able to provide a view of access levels for all staff members at any one time, including any periods of inactivity

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

Queried Processor access to personal data

---

## 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.

---

## 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."]					



---

## INTERNATIONAL TRANSFERS

---

Query which jurisdictions have been selected for AWS.

---

## 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
- Amazon Web Services have submitted a compliant NHS Data Protection and Security Toolkit for the current year available at [AWS Toolkit](#)
- Amazon Web Services has achieved ISO27001 accreditation as confirmed via [AWS 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, aside from Amazon, no stakeholders had no media presence with regards to data breaches.

The ICO have not released any formal advice to indicate that AWS are not a suitable provider for services.

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
- Amazon Web Services are registered with the ICO under the registration number ZA481902

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

- Prescribing Services Ltd - Emma Cooper - [emma.cooper@kafico.co.uk](mailto:emma.cooper@kafico.co.uk)

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.