Data Protection Impact Assessment

Community and Inpatient CQUIN 2018/19

Document Information

Title of document	Data Protection Impact Assessment
Version number	1.1
Type of document	Template for Assessment
Purpose of document	To capture the impact of project related data collection including pseudonymised, special category (sensitive), healthcare, social care, financial (this list is not exhaustive).
Target audience	All College staff and contractors
Distribution	Intranet (electronic)
Consultation	Interim Director of Information Services. GDPR Project Steering Group
Approved by	Richa Kataria, Interim Data Protection Officer
Date of approval	July 2018
Author	Kathryn Campling GDPR Consultant
Review date	2 years or sooner is required

Document Control

Version Number	Reason for Change	Description of Change	Date of Change	Author
Draft	Original draft	Creation	June 2018	Kathryn Campling GDPR Consultant
V1.1	Amendments to include Table of contents, cover page, document control, tables and risk register annex 3	Updates	June 2018	Susie Griffin GDPR Project Manager

Contents

Data Protection Impact Assessment

Overview

If you're conducting a project that will use personally-identifiable information, whether you're collecting it or it is being given to you, or you want to use an existing store of data in a different way; you must now consider completing a *Data Protection Impact Assessment* (DPIA). The sort of personal data which will attract a DPIA are: pseudonymised, special category (sensitive), healthcare, social care, financial (this list is not exhaustive). For more information on anonymisation/pseudonymisation please see the references section at the end of this document.

This document comprises two sections:

1. A set of screening questions, for people who are unsure whether or not they need to fill in a DPIA
2. A template form for a DPIA, based on guidance issued by the Information Commissioner's Office (ICO). This form walks you through all the issues you need to consider when conducting a PIA

Please read and complete the DPIA alongside Annex 2 which includes the Data Processing Principles from the GDPR.

Section 1: Screening questions

These questions are intended to help you decide whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. You should consider completing a DPIA for projects which are already running where the screening questions can be applied. You can expand on your answers as the project develops if you need to:

1. Will/does the project involve the collection of new information about individuals? Re-use of data collected for a different purpose is covered by question 4.	Yes – pseudonymous data
2. Will/does the project compel individuals to provide information about themselves or ask others to disclose it on their behalf? (e.g. a Trust providing data about an individual patient's care?)	Yes – for the purpose of commissioning for Innovation and quality improvement, the project requires participating services (Trusts, specialist mental health services) to provide clinical data on the care of individual service users.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes – pseudonymous data are collected via and online tool provided by a third party supplied (Formic Solutions).
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	Yes – data to be sent to NHS England for the purpose of calculating CQUIN payments.
5. Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. This would cover things like fingerprint technologies.	No
6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	No

7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private. Or any of the sensitive personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life.	Yes - sensitive pseudonymous data are collected relevant to an individual's care under mental health services, such as their age, gender, ethnicity, diagnosis, clinical setting, physical health assessment and intervention where required.
8. Will the project require you to contact individuals in ways that they may find intrusive?	No
9. Does the project involve any data concerning vulnerable individuals who may be unable to easily consent or oppose the processing, or exercise their rights? This group may include children, employees, mentally ill persons, asylum seekers, or the elderly, patients and cases where there is an imbalance in the relationship between the position of the individual and the controller.	Yes – services users under the care of mental health services
10. Does your project collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing')?	Yes – pseudonymous service user data are collected from participating members of the project. Only participating services are provided with our online privacy notice

Section 2: Data Protection Impact Assessment Form

Step one: Identify the need for a DPIA

Explain what the project aims to achieve, what the benefits will be to the College, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a DPIA was identified drawing on your answers to the screening questions.

The Commissioning for Quality and Innovation (CQUIN) framework aims to support improvements in the quality of services and create new improved patterns of care. One of the CQUIN goals for 2018/19 is to improve the physical healthcare of people with severe mental illness. It aims to support NHS England's commitment to reduce the 15 to 20 year premature mortality in people with severe mental illness and improve their safety through improved assessment, treatment and communication between clinicians.

NHS England has commissioned the CCQI to manage the data collection process for part 3a of the mental health CQUIN, which focuses on all patients with psychoses, including schizophrenia and bipolar affective disorder, including both inpatient and community patients in all NHS commissioned sectors including the independent sector.

Data are collected locally by participating services from local patient records, which are then supplied to the CCQI CQUIN team via an online data collection tool. The CCQI CQUIN team then return to each participating service their own data via a password protected spreadsheet. Services then have 15 days to provide the CCQI with any amendments. The CCQI CQUIN team then analyse the data and provide this to NHS England to determine whether CQUIN thresholds are met. NHS England disseminate CQUIN results to services. The CCQI CQUIN team provides each participating service with their final, amended data set.

The data collected are pseudonymous but comprise sensitive information relevant to an individual's care under mental health services (such as age, gender, ethnicity, diagnosis, and treatment details). These service user data are provided to the project by Trust/healthcare organisations on their behalf. As we are collecting pseudonymous data as part of a clinical audit for the purpose of quality improvement and patient care, explicit patient authorisation for sharing these data is not required. However, for reasons outlined in section 1, such as the potential privacy concerns of these sensitive data, relating to individuals who may be considered vulnerable, a DPIA is warranted.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows – where you are getting the data from, where it will be stored and where it could be transferred to. You should also say how many individuals are likely to be affected by the project. Please ensure you identify the Data Controller and Data Processor/s within the flows and any sub-contracted parties.

Data flow

Data controller	The CCQI CQUIN team develops the audit tool in accordance with NHS England requirements. The audit tool is released and data are requested from members
	↓
Data processor and source	Members submit pseudonymous data online using Formic solutions data collection tool
	↓
Data processor	Pseudonymous data are stored on Formic Solutions servers
	↓
Data controller	Pseudonymous data are downloaded by the CCQI CQUIN team and stored on RCPsych server
	↓
Data controller	The CCQI CQUIN team emails participating services with their own submitted datasets as password protected documents for local checking and amendment.
	↓
Data processor and source	Participating services send any data amendments to the CCQI CQUIN team
	↓
Data controller	Pseudonymous data are accessed on servers by project team and analysed using computer software (2-3 people)
	↓
Data controller	CCQI CQUIN team analyses data and sends this to NHS England via password protected spreadsheets
Data controller	CCQI CQUIN team sends participating services their own final amended data sets.
	↓
Data controller	CCQI deletes datasets from Formic data collection system once reporting has been completed

Summary

	Service user personal and healthcare records
Data source:	NHS Trusts and CCG commissioned private mental health care providers via online portal
Output:	Datasets in SPSS and Excel for cleaning and analysis
Data shared with:	CCQI CQUIN team (pseudonymous data) Member Trusts/local audit teams (pseudonymous data)
Contains identifiable personal information?	Yes (pseudonymous data only). Datasets contain a unique personal identifier that corresponds with additional personal records held by the Trust/healthcare organisation
Contains sensitive information?	Yes - clinical information related to the individual's care under mental health services
Electronic Storage:	Yes - **RCPsych** - Datasets are held on college servers. Computers are password protected and access is restricted to specified members of the CCQI CQUIN team. Any datasets shared by email are password protected. Any laptops used to store or transport data are supplied by the college with appropriate security and password protection. **Formic solutions** - Datasets are held by this third party supplier until deleted by the CCQI CQUIN team. Formic hold the following security credentials: ISO27001:2013 Certified, Cyber Essentials Plus Certified, IGSoC (IG Toolkit) level 2 attainment.
Paper/Hard copy storage:	Blank copies of the audit materials only.
Comments:	

In addition to the sensitive pseudonymous data outlined above, service contact names, telephone numbers and email addresses are collected for the purpose of administering the project. All such contact details are retained on college servers. Computers are password protected and access is restricted to specified members of the CCQI CQUIN team.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address Data Protection risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the DPIA process.

e.g. Discussed storage with Information Security Team.

- Discussed College IG policy and data management processes with project team
- Discussed GDPR requirements with internal Data Protection team and GDPR leads

Step three: Identify the Data Protection and related risks

Identify the key Data Protection risks and the associated compliance and corporate risks.

Privacy issue	***Risk to individuals***	***Compliance risk***	***Associated organisation / corporate risk***
Sensitive pseudonymous data is collected on thousands of service users, which is copied across software files for cleaning/analysis	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	As data are pseudonymous, Subject Access would need to be referred to the originating service.	Could lead to regulatory fines, reputational damage.
Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts during data collection	Sensitive data relating to an individual's mental health is linked to identifying data, which could cause harm or distress if shared	The project accumulates personal, excessive data without purpose or appropriate controls. The impact of any data breach is increased	Could lead to regulatory fines, reputational damage.
Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Pseudonymous data held on third party servers (Formic Solutions)	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data is copied and/or retained longer than required, is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.
Datasets shared by email	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data is subject to unlawful access or processing, if lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.

Laptop containing pseudonymous data that is lost or stolen	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage
The wrong datasets are shared with members, containing data on service users from other organisations	Personal, sensitive data, relating to an individual's mental health, could cause harm or distress if accessed/shared/ lost	Data is subject to unlawful access or processing, or is lost or shared as part of a data breach	Could lead to regulatory fines, reputational damage.

Step four: Identify solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems). Risks may include those affecting individuals, organisations or third parties (e.g. misuse or overuse of data, loss of anonymity etc.), compliance risks with GDPR or other relevant legislation, corporate risks (e.g. reputational, loss of trust of service users or the public).

Risk: use the Corporate Risk Matrix to calculate a score based on likelihood and impact (Annex 3)	***Solution(s)***	***Result:** is the risk eliminated, reduced, or accepted?*	***Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?*
1. Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts the sampling period **Risk score: 8**	Sampling forms include clear warnings against supplying excessive and unnecessary personal data. A process is in place to notify services of any breach and to double delete relevant data.	**Risk is reduced**	**Impact is justified:** Opportunities to submit unwanted data are reduced but still exist. These are necessary for the accuracy and completeness of reporting.
2. Pseudonymous data held on third party servers (Formic Solutions) **Risk score: 8**	CCQI CQUIN team is able to use Formic's online system to delete data retained, once no longer required. Contract is in place with Formic, who appropriate hold security credentials: (ISO27001:2013 Certified, Cyber Essentials Plus Certified, IGSoC (IG Toolkit) level 2 attainment)	**Risk is reduced**	**Impact is justified:** Third party supplier is required for the specialised IT system and management of large data submissions

3. Datasets shared by email **Risk score: 8**	All shared datasets are password protected. Datasets containing unique identifiers are only shared with the data source (participating services). Data emailed are otherwise made anonymous.	**Risk is reduced**	**Impact is justified:** Datasets are emailed to members for essential data cleaning and local analysis.
4. Laptop containing pseudonymous data that is lost or stolen **Risk score: 6**	Only college approved laptops are used with appropriate security protections.	**Risk is reduced**	**Impact is justified:** Storage and use of data on laptops supports project workflow.
5. The wrong datasets are shared with members, containing data on service users from other organisations **Risk score: 6**	All shared datasets are password protected.	**Risk is reduced**	**Impact is justified:** Datasets are emailed to members for essential data amendments and local analysis.
6. Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych **Risk score: 4**	Datasets are stored on secure servers with restricted access to project folders. Computer terminals time-out and require password access.	**Risk is reduced**	**Impact is justified:** Extent of staff access to data stored electronically is the minimum necessary for the delivery of project aims.
7. Sensitive pseudonymous data is	Policy is to review retention of datasets annually.	**Risk is reduced**	**Impact is justified**:

collected on thousands of service users, which is copied across software files retained for five years. **Risk score: 4**	After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers. Datasets are stored on secure servers with restricted access.		Pseudonymous data are retained to ensure resolution of queries. validity of reporting. Copying datasets is essential for the stages of data cleaning, analysis

Step five: Sign off and record the DPIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Person Responsible and deadline for completion	Approved by
Personally identifiable service user data (e.g. NHS number, full date of birth) may be mistakenly shared by Trusts during data collection	Sampling forms include clear warnings against supplying excessive and unnecessary personal data.	Krysia Zalewska Programme Mgr. *Completed*	Alan Quirk, Senior Programme Mgr.
	Online forms are designed with restricted fields to reduce errors.	Krysia Zalewska, Programme Mgr. *Completed*	Alan Quirk, Senior Programme Mgr.
Pseudonymous data held on third party servers (Formic Solutions)	The CCQI CQUIN team is able to use Formic's online system to delete data retained, once no longer required.	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.
	Contract is in place with Formic, who hold appropriate security credentials.	Chris Lord, Head of IT *Completed*	Alan Quirk, Senior Programme Mgr.
	CCQI CQUIN team unique passwords to access Formic are changed on a regular basis	Krysia Zalewska, Programme Mgr. *Ongoing activity*	Alan Quirk, Senior Programme Mgr.
Datasets shared by email	All shared datasets are password protected.	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.

	Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous.	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.
Laptop containing pseudonymous data that is lost or stolen	Only college approved laptops are used with appropriate security protections	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.
The wrong datasets are shared with members, containing data on service users from other organisations	All shared datasets are password protected, with a unique password per service. Passwords are not sent with datasets. Emails containing datasets are cross checked by another member of the CCQI CQUIN team.	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.
Pseudonymous data (electronic or printed) accessed by unauthorised staff at RCPsych	Datasets are stored on secure servers with restricted access to project folders. Computer terminals time-out and require password access.	Chris Lord, Head of IT *Completed*	Alan Quirk, Senior Programme Mgr.

Sensitive pseudonymous data is collected on thousands of service users for each audit, which is copied across software files retained indefinitely for long-term statistical analysis	Policy is to review retention of datasets annually.	Krysia Zalewska, Programme Mgr. *Completed and ongoing activity*	Alan Quirk, Senior Programme Mgr.
	After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Krysia Zalewska, Programme Mgr. *28 February 2019*	Alan Quirk, Senior Programme Mgr.
	Datasets are stored on secure servers with restricted access.	Chris Lord, Head of IT *Completed*	Alan Quirk, Senior Programme Mgr.

Step six: Integrate the DPIA outcomes back into the project plan

Who is responsible for integrating the DPIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any Data Protection concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Sampling forms include clear warnings against supplying excessive and unnecessary personal data.	Completed	Krysia Zalewska and Richa Kataria (Acting DPO)
Online forms are designed with restricted fields to reduce errors.	Completed	Krysia Zalewska and Richa Kataria (Acting DPO)
CCQI CQUIN team is able to use Formic's online system to delete data retained, once no longer required.	Ongoing	Krysia Zalewska and Richa Kataria (Acting DPO)

Contract is in place with Formic, who appropriate hold security credentials.	Completed.	Krysia Zalewska and Richa Kataria (Acting DPO)
All shared datasets are password protected.	Completed.	Krysia Zalewska and Richa Kataria (Acting DPO)
Datasets containing unique identifiers are only shared with the data source (member organisations). Data emailed are otherwise made anonymous.	Ongoing	Krysia Zalewska and Richa Kataria (Acting DPO)
Only college approved laptops are used with appropriate security protections	Completed.	Krysia Zalewska and Richa Kataria (Acting DPO)
All shared datasets are password protected.	Ongoing	Krysia Zalewska and Richa Kataria (Acting DPO)
Datasets are stored on secure servers with restricted access to project folders. Computer terminals time-out and require password access.	Completed.	Krysia Zalewska and Richa Kataria (Acting DPO)
Policy is to review retention of datasets annually.	Ongoing	Krysia Zalewska and Richa Kataria (Acting DPO)
After being held for 5 years, pseudonymous data will be made anonymous by deletion of unique patient identifiers.	Ongoing	Krysia Zalewska and Richa Kataria (Acting DPO)
Datasets are stored on secure servers with restricted access.	Completed.	Krysia Zalewska and Richa Kataria (Acting DPO)

Contact point for future privacy concerns
Richa Kataria, Acting Data Protection Officer

Annex 1

Primary contact for advice and guidance

Richa Kataria
Head of Membership Operations – Acting Data Protection Officer
richa.kataria@rcpsych.ac.uk
020 3701 2589

Annex 2

The data protection principles and relevant questions

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the General Data Protection Regulation, Data Protection Act 2018 or other relevant legislation, for example the Human Rights Act.

Personal data shall be:

1. **processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');**

    a) Have you identified the purpose of the project?

    b) How will you tell individuals about the use of their personal data?

    c) Do you need to amend or create a new privacy notice/s?

    d) Have you established which conditions for processing apply?

    e) If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

    f) If your organisation is subject to the Human Rights Act, you also need to consider:

    g) Will your actions interfere with the right to privacy under Article 8?

    h) Have you identified the social need and aims of the project?

    i) Are your actions a proportionate response to the social need?

2. **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89 (1), not be considered to be incompatible with the initial purposes ('purpose limitation');**

    a) Does your project plan cover all of the purposes for processing personal data?

    b) Have you identified potential new purposes as the scope of the project expands?

    c) Consider using the Data Categories table at Annex 4 to help you identify the purposes of your collection/processing – this may help you evaluate the scope of the data required for your project.

3. **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');**

    a) Is the quality of the information good enough for the purposes it is used?

    b) Which personal data could you not use, without compromising the needs of the project?

4. **accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');**

    a) If you are procuring new software does it allow you to amend data when necessary?

    b) How are you ensuring that personal data obtained from individuals or other organisations is accurate?

5. **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');**

    a) What retention periods are suitable for the personal data you will be processing?

    b) Are you procuring software that will allow you to delete information in line with your retention periods?

6. **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 ('integrity and confidentiality').**

    a) Do any new systems provide protection against the security risks you have identified?

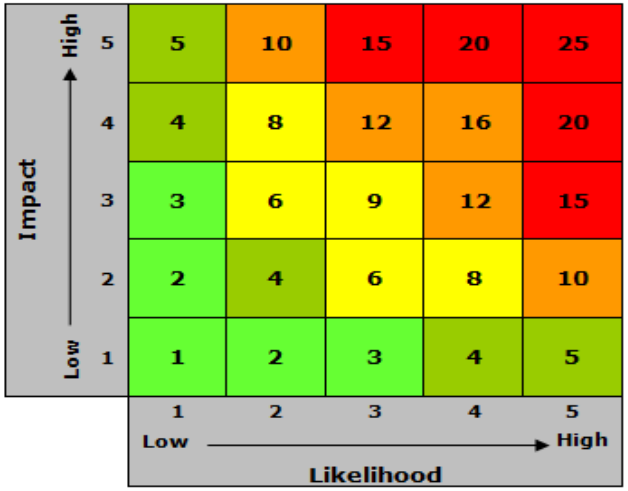
    b) What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Annex 3

Risk and Issues Log

Risk No	Risk Description	Likeli-hood	Severity of Impact	Raw Risk Score	Mitigation	Likelihood	Severity of impact	Residual Risk	Owner
1				8					
2				8					
3				8					
4				6					
5				6					
6				4					
7				4					

1-3	Low likelihood & low severity of impact
4-5	Low / medium likelihood & low / medium severity of impact
6-9	Medium likelihood & medium severity of impact
10-16	Medium / high likelihood & medium / high severity of impact
15-25	High likelihood & high severity of impact



Annex 4

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name		✓	
NHS number		✓	
Address		✓	
Postcode		✓	
Date of birth		✓	
Date of death		✓	
Age	✓		Demographic data to inform analysis and quality improvement
Sex	✓		Demographic data to inform analysis and quality improvement
Marital Status		✓	
Gender	✓		Demographic data to inform analysis and quality improvement
Living Habits		✓	
Professional Training / Awards		✓	
Income / Financial / Tax Situation		✓	
Email Address		✓	
Physical Description		✓	
General Identifier e.g. Hospital No/Paris ID		✓	
Home Phone Number		✓	
Online Identifier e.g. IP Address/Event Logs		✓	
Website Cookies		✓	
Mobile Phone / Device No		✓	
Device Mobile Phone / Device IMEI No		✓	
Location Data (Travel / GPS / GSM Data)		✓	
Device MAC Address (Wireless Network Interface)		✓	

Data Categories [*Information relating to the individual's*]	**Is this field used?**	**N / A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Sensitive Personal Data			
Physical / Mental Health or Condition	✓		
Sexual Life / Orientation		✓	
Family / Lifestyle / Social Circumstance		✓	
Offences Committed / Alleged to have Committed		✓	
Criminal Proceedings / Outcomes / Sentence		✓	
Education / Professional Training		✓	
Employment / Career History		✓	
Financial Affairs		✓	
Religion or Other Beliefs		✓	
Trade Union membership		✓	
Racial / Ethnic Origin	✓		Demographic data to inform analysis and quality improvement
Biometric Data (Fingerprints / Facial Recognition)		✓	
Genetic Data		✓	
Use of Mental Health Legislation/DoLS etc.		✓	Clinical data to inform analysis and quality improvement
Care Data including interventions, procedures, surgery etc.	✓		Clinical data to inform analysis and quality improvement