Privacy Impact Assessment

CPH004 Inpatient Treatment for the Management of Withdrawal from Drug and Alcohol Dependence

APPENDIX A

Privacy Impact Assessment – Screening Questions

Question	Y/N	Additional Comments (please give reasons for either a 'yes' or' no 'answer here
Is there a requirement under GDPR to carry out a PIA? NB if there is a legal requirement to carry out a PIA there is no requirement to complete the remaining questions.	N	This is a review of existing systems and processes for the re-procurement of the service which has been running for 4 years. Processing special category and sensitive data is low risk as appropriate measures are in place to protect and safeguard individuals data and therefore does not pose a risk to the rights and freedoms of the individual.
Will the project involve the collection of new information about individuals?	Y	The project is being re-procured and a PIA is being carried out to ensure data processing complies with GDPR. The provider will be receiving sensitive data from the community treatment service and will be collecting data from the patient when being assessed.
Will the project compel individuals to provide information about themselves?	Y	Clients are required to give personal and sensitive data in order to receive the service.
Will information about individuals be disclosed to third party organisations or people?	Y	The inpatient treatment centre will not be disclosing any new data that the community treatment centre and residential rehab are not already aware of.
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
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.	N	

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	Y	The Council may refuse funding the placement. The provider may discharge the patient before completion of treatment.
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union information, biometric data, health or information concerning an individual's sex life or sexual orientation or other information that people would consider to be private.	Y	Personal and sensitive data will be collected
Will the project require you to contact individuals in ways that they may find intrusive?	N	Individuals have chosen how they wish to be contacted.
Will the data be held in relation to children or vulnerable adults?	Y	Personal and sensitive data will be held by the provider.

APPENDIX B

Privacy Impact Assessment

Step 1 – Requirement for PIA – issues to be addressed

To Include:

Project Aim: The service aims to medically manage withdrawal from drug and alcohol dependence, or stabilise opiate substitution therapy, in an inpatient setting

Objectives:

- To provide a comprehensive assessment of the patient's need with regard to severity of dependence, physical and mental health co-morbidity, and social situation, in order to determine suitability for inpatient treatment.
- To comprehensively assess risks associated with withdrawal and to manage those risks
- To provide supervised medication to prevent or ease withdrawal symptoms
- To deliver psycho-social interventions to compliment pharmacological treatment and support sustainable recovery

Benefit: While most drug or alcohol dependent patients can successfully complete drug or alcohol withdrawal with the assistance of the community treatment service, there are some patients for whom inpatient managed withdrawal is required. These include:

- Patients who present with significant comorbid physical or mental health problems

- Patients with a history of severe withdrawal symptoms, including seizure activity
- Patients with complex poly-drug and alcohol misuse
- Patients who have failed previous community-based attempts at withdrawal
- Patients with little or no social support in the community

Requirement for a PIA: Personal and sensitive data will be collected to enable clients to be referred to the relevant treatment centres. The Council is performing a PIA to ensure the re-procurement of the service is compliant with GDPR requirements and to ensure privacy risks are minimised.

Step 2 – Information Flows/Nature of processing

To Include:

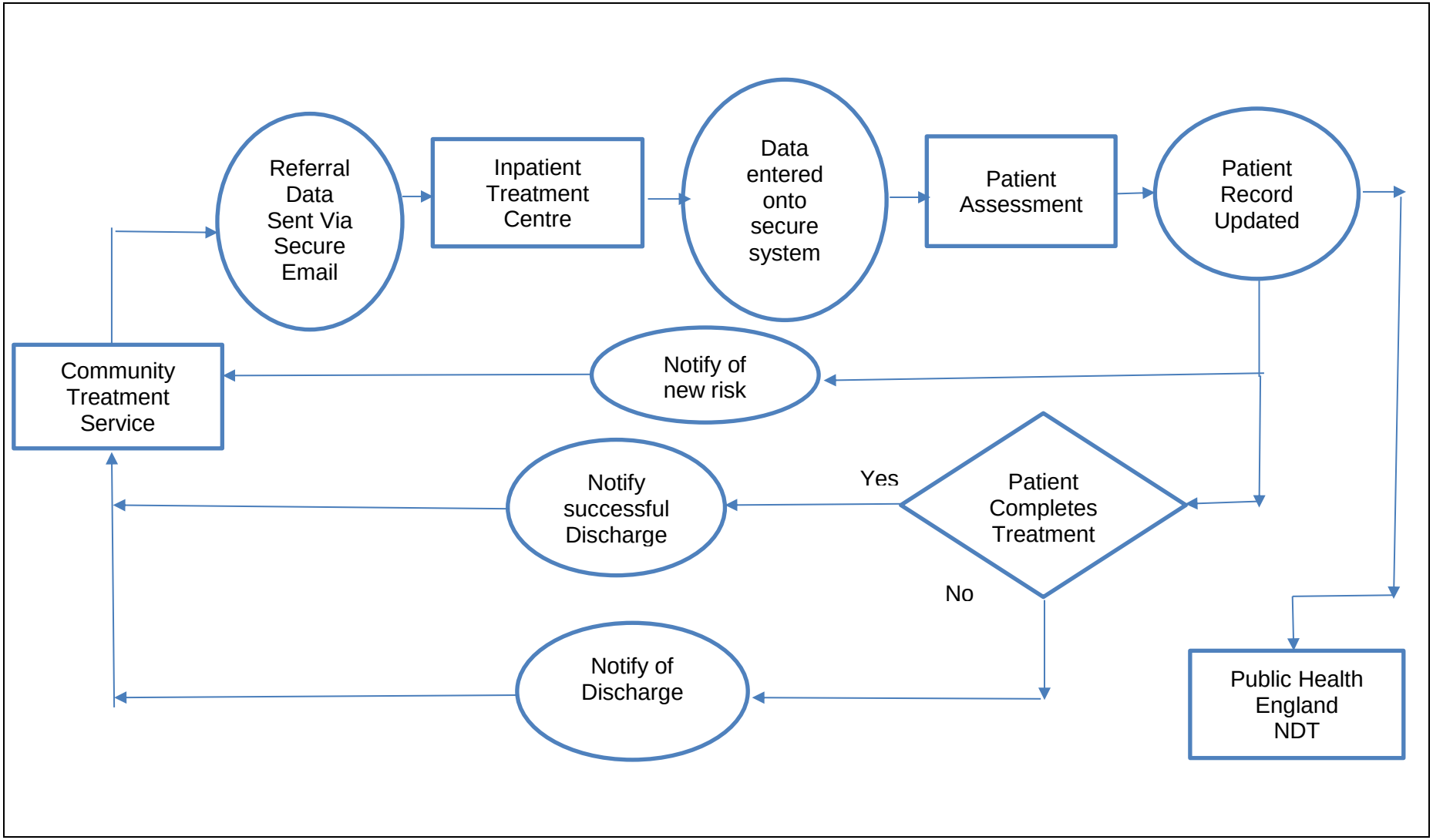
Community Treatment Service (Data Controller) – send referral document by secure email NHS.net or secure encryption to provider Inpatient Treatment Centre which will contain patient sensitive and special category data.

See attached referral forms completed by the Community Treatment Centre and via secure email to Inpatient Treatment Centre.

Data Transmitted
Name
Address
Dob
Gender
Ethnicity
Sexuality
GP
Substance misuse history.
Mental Health history
Physical Health
Current medication
Risk assessment

Provider Inpatient Treatment Centre (Data Processor) – will assess patient and obtain and record additional data (see referral forms attached): Substance misuse history.
Mental Health history
Physical Health

See information flow diagram on next page.


Referral Data Sent Via Secure Email
Inpatient Treatment Centre
Data entered onto secure system
Patient Assessment
Patient Record Updated
Community Treatment Service
Notify of new risk
Notify successful Discharge
Yes
Patient Completes Treatment
No
Notify of Discharge
Public Health England NDT

Reason for Processing - Data is only processed for legitimate interests and the lawful basis for processing special category data is for the provision of providing patients with the relevant treatment.

Numbers of Patient – Currently receiving treatment across 3 providers, 60 patients per annum.

Data Security – Providers have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. Access to personal data is limited to employees who's role requires access for service and treatment purposes. Data security requirements are covered in the contractual arrangements and compliance with Audits requirements with regards to information security.

International Transfers – Personal data will not be transferred or stored outside of the UK.

Patient Discharge – Provider Inpatient Treatment Centre (Data Processor) will notify Community Treatment service of discharge by secure email.

Data Retention - Providers will only retain personal data for as long as necessary to fulfil the purposes it is collected for, including the purposes of satisfying any legal, accounting or reporting requirements.

Current National companies data retention periods.

Data relating to Health – Period of 8 years from end date of treatment.

Data relating to Controlled Drugs records – Period minimum of 2 years and a maximum of 7 years.

Data relating to Contractual Data – Period of 6 years from the end date.

NHS bodies will retain record in line with NHS data retention regulations – see attached.

Step 2 – Consultation Requirements

Procurement - Providers will be required to obtain Cyber Essentials or equivalent unless accredited to IS27001 as per the Selection Questionnaire in procurement documentation.

DCC Audit Services - will be required to undertake an Information Security Audit and ISO27001:2013 audit of the 3 – 4 Inpatient Treatment Centre providers to ensure compliance with GDPR.

Audit Services to establish Inpatient Treatment Centres have the appropriate levels of security in place to manage, protect and safeguard patient information. To report on findings of potential non-conformities for the provider to consider findings and agree a timetable for correction. Prior to final report being referred to the County Councils Director of Finance and ICT for consideration.

Part B Steps 3 to 4 – Identify Privacy Risks, Solutions and Approval

Privacy Risk	Risk to Individuals & organisation	Risk initial score include mitigations as it is an existing service	Action Identified	Target Score (after applying actions)	Risk Control Plan (Treat/Control/Tolerate/Accept/Terminate/Transfer)	Evaluation: is the final impact on individuals and the organisation after implementing each solution a justified, compliant and proportionate response to the aims of the project?	Approved By
Disclosure of the personal sensitive data that is require to deliver the service.	Harm and distress if released, unauthorised access or used for different purposes Inappropriate/excessive disclosure of personal and sensitive data. Financial and reputational damage. Legal action	1x 4 =4	Compliance with DPA laws. Providers have procedures, protocols and policies in place for staff to comply with. Information Security Audit from DCC will be required.	4	Treated/Control	Yes- all other solutions were implemented 4 years ago when contract commenced, apart from Security Audit.	
Data is accessed by	Risks to the individual as a	1x 4 =4		4	Treated/Control	Yes- all other solutions were	

unauthorised persons and used or shared inappropriately	result of contravention of their rights in relation to privacy, or loss, damage, misuse or abuse of their personal information Financial and reputational damage. Legal action					implemented 4 years ago when contract commenced, apart from Security Audit.	
Data held for longer than lawful retention period	Data is kept longer than is necessary.	1 x 1 = 1	Provider ensures staff are trained and comply with retention policy.	1 x 1 =1	Treated/Control	Yes- all other solutions were implemented 4 years ago when contract commenced, apart from Security Audit.	

Step four: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA 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 privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Inform Key Stakeholders of PIA outcomes	14.01.19	Nik Howes
Update Audit	14.01.19	Nik Howes and Jayne Smith
Contractual Requirements	14.01.19	Nik Howes and Jayne Smith

Contact point for future privacy concerns
Nik Howes
Date of consideration by IGG

APPENDIX C

Linking the PIA to the GDPR principles

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

Principle 1

Personal data shall be processed fairly and lawfully

There must be lawful basis for processing the personal data as follows;

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(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.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? | e |
- Is the processing of the data necessary in terms of GDPR? | Y |
- How will you tell individuals about the use of their personal data?

Providers will obtain consent from the Patient, completing a consent form.

- Do you need to amend your privacy notices? – Council
- Providers Privacy notices have been updated - Yes | N |
- 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? Council | N |

- Providers have updated their consent forms - Yes
- If special categories of personal data have been identified have the requirements of GDPR been met? | Y |

As the Council subject to the Human Rights Act, you also will where privacy risk are especially high need to consider:

- Will your actions interfere with the right to privacy under Article 8? | Y |
- Have you identified the social need and aims of the project? | Y |
- Are your actions a proportionate response to the social need? | Y |

Principle 2

Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Does your project plan cover all of the purposes for processing personal data? | Y |
- Have you identified potential new purposes as the scope of the project expands? | N |
- Does your Privacy Notice cover all potential users? | Y |

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- Is the quality of the information good enough for the purposes it is used? | Y |
- Which personal data could you not use, without compromising the needs of the project?

None

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

- If you are procuring new software does it allow you to amend data when necessary? (Not procuring software) | N |
- How are you ensuring that personal data obtained from individuals or other organisations is accurate? Through contractual requirements, collecting data for the sole purpose of the service and ensuring the data is maintained and accurate. | |

Principle 5

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

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

Provider Retention periods Health – Period of 8 years from end date of treatment. Controlled Drugs records – Period minimum of 2 years and a maximum of 7 years

- Are you procuring software that will allow you to delete information in line with your retention periods? Not procuring software, however providers systems have the functionality for data to be deleted. | N |

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under GDPR.

- Will the systems you are putting in place allow you to respond to subject access requests more easily? Contractual requirements are in place to comply. | Y |

- Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and the right to ensure (right to be forgotten). Contractual requirements are in place to comply. | Y |

- If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose? There is no marketing involved in the contract. | N |

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Do any new systems provide protection against the security risks you have identified? | N |

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

The procurement is not for a new system, it is to deliver a service. The Providers, provide appropriate training is given to staff to ensure data is kept safe e.g. password kept safe and not shared, locking screens and logging out of systems, only accessing records when required.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- Will the project require you to transfer data outside of the EEA? N
- If you will be making transfers, how will you ensure that the data is adequately protected?

Not applicable