Appendix A

PRIVACY IMPACT ASSESSMENT

(Insert project name)

PART 1: SCREENING QUESTIONS

Please see below the non-exhaustive list of situations where a PIA is likely to be necessary. If your project involves the use of personal data and is not included in the list, please seek further advice from the Information Governance Department (IG).

If the answer is yes to any of these questions move to Step 2 and complete a PIA.

Project	Yes / No
Will the project involve the collection of new information about individuals?	
Will the project compel individuals to provide information about themselves?	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Do you intend to use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
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.	
Will the project result in you making decisions or taking actions against individuals in ways that can have a significant impact on them?	
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.	
Will the project require you to contact individuals in ways that they may find intrusive?	

PART 2: COMPLETE THE PIA

Step one: Identify the need for a PIA
What does the project aim to achieve? (attach any relevant documents)
(please refer to 4.2.1 on the PIA procedure)
What are the benefits to the organisation? (attach any relevant documents)
(please refer to 4.2.2 on the PIA procedure)
State the name of the Information Asset Owner and Information Asset Administrator and confirm that asset will be added to the register on completion.
(please refer to 4.2.3 on the PIA procedure)

Step two: Describe the information flows
What data will be collected? (E.g. demographic, medical record (diagnostic/therapeutic), biometric, personal financial, ID number, location data, IP address, cookie address, cultural & social)
(please refer to 4.2.4 on the PIA procedure)
How is the data collected? Please use a diagram if necessary.
(please refer to 4.2.5 on the PIA procedure)
What is the legal basis for the collection of this new information? (E.g. consent by data subject, performance of contract to which data subject is party; compliance with legal obligation; research; performance of a task carried out in the public interest; protection of vital interests of data subject)

(please refer to 4.2.6 on the PIA procedure)

If consent is the legal basis for the use of the data, how is it obtained?
Does the consent form require some positive, affirmative action?
What information has been given to the data subject prior to consent being obtained?
How has the consent by the data subject been recorded?
Attach a copy of the consent form and any guidance leaflets where applicable.

(please refer to 4.2.7 on the PIA procedure)

Is personal data of children being used? If so, has parental permission been obtained for the use of this information? (N.B. The GDPR does not prescribe the age at which a person is considered to be a child. However, Art 8 GDPR states that 'information society services which are offered directly to a child shall be lawful where the child is at least 16 years old. Individual member states are at liberty to lower this age to 13.)
Has the privacy notice been written in clear, plain language which a child can understand?

(please refer to 4.2.8 on the PIA procedure)

Has the data subject been informed about:

- **Purposes of the processing?**
- **Contact details of the data protection officer?**
- **Rights to access, withdraw, delete and/or rectify the data collected? (N.B. the right to 'delete' personal data does not apply to 'health data')**
- **<u>How</u> these rights can be exercised (email address/ telephone number)?**
- **<u>When</u> these rights can be exercised (i.e. following the applicable retention period?**
- **How to lodge a <u>complaint?</u>**
- **<u>List/categories</u> of recipients of data?**

(please refer to 4.2.9 on the PIA procedure)

What checks have been made to ensure you are collecting the minimum amount of data necessary for the project?

(please refer to 4.2.10 on the PIA procedure)

Who will have access to the data, for what purpose and what access controls will be in place?

(please refer to 4.2.11 on the PIA procedure)

What audit system is in place to assess who has accessed the data?

(please refer to 4.2.12 on the PIA procedure)

How have the information security risks been assessed? Please include details of at least the following:

- **Technical Security**
  - **access control (guests, regular users, administrators or super users, etc.)**
  - **password complexity**
  - **automatic user suspension**
  - **auto-log-off or screen lock function**
  - **remote access capability**
  - **audit trail (including 'read/view' access; 'creation/modification/deletion of data' and 'import/export of data from removable media')**
  - **external communication capability**
- **Physical Security**
- **Data recovery / Business Continuity**
- **Encryption Facilities (server, database, email, file, removable media etc.)**
- **Network security management (Cloud considerations)**
- **Penetration Tests for external-facing systems**
- **Emergency Access ('Break Glass' feature)**
- **Malware Protection/Detection**
- **Privacy and security monitoring and reporting function**
- **Security incident response plan**
- **User education and training**
- **Health data integrity and authenticity**
- **Cyber Security Product Upgrades for third party systems (Who has the**

ability to install/upgrade the system's security patches: IT service desk staff; TP staff with physical on-site access or remote access?)

(please refer to 4.2.13 on the PIA procedure)

Will any data be transferred outside the UK? Please provide details.

(please refer to 4.2.14 on the PIA procedure)

How will the data be kept up-to-date and accurate?

(please refer to 4.2.15 on the PIA procedure)

What action is being taken to ensure the quality of the data? Please include details of the training which will be given to users of the system to ensure they meet this requirement.

(please refer to 4.2.16 on the PIA procedure)

How long will the data be retained for?

(please refer to 4.2.17 on the PIA procedure)

Consultation requirements (please refer to 4.2.18 on the PIA procedure)

Who do you need to consult to identify and address any privacy risks?

How will you carry out the consultation? Please link to Project Management plan if necessary.
Consultation with IT (yes/no/provide details) Consultation with Informatics (yes/no/provide details)

Step three: Identify the privacy and related risks (please refer to 4.2.19 on the PIA procedure)
Use Trust Information Risk Assessment Template (Appendix B) and Risk Matrix (Appendix C).

Step four: Integrate the PIA outcomes back into the project plan (please refer to 4.2.19 on the PIA procedure)		
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**

PART 3: RECOMMENDATIONS BY IG

Recommendation	
Name	
Job Title	
Date	

PART 4: APPROVAL BY DHG OR IGG

Comments (if any)	
Name	
Job Title	
Date	

Appendix 1 Risk Assessment **Date:**

Name or Project:

What are the risks? (*Nature of Risk)*	**Potential impact?**	**What are you already doing? *(Control Name & Assurance Source)***	**Estimate of "Risk Significance?"**			**What further actions are necessary? *(Action Plan)***	**Who is responsible for executing action plans?**		
Examples: – *Theft – internal or external* – *Loss/destruction such as accidental loss of a copy by a person, accidental loss of an original by a person, destruction due to flooding, fire, etc;* – *Unauthorised access such as accidental access by staff (paper copies left unsecure, PCs left unlocked, etc), accidental access by others (paper copies left unsecure, PCs left unlocked, etc); deliberate unauthorised access (i.e. password issues); deliberate hacking attack;* – *Errors/Inaccuracies such as small scale error; widespread error, deliberate modification*	*Consider the extent and nature of harm:* – *Unavailability of data* – *Clinical safety* – *Administrative disruption* – *Inappropriate disclosure to staff or external parties* – *Reputation & financial damage*	*List what is already in place to reduce the likelihood or seriousness of impact.* *Example: Secure destruction of paper records upon lapse of retention period; use of passwords/log-ins; audits; etc.*	*Using the Trust risk matrix for likelihood & consequence. Multiply to get risk rating.*			*You need to make sure that you have reduced risks 'so far as reasonably practicable'.*			
			C	**L**	**CxL**		**Action by whom**	**Action by When**	**Done**
									☐
									☐

									☐
									☐

Review date:		• *Review intervals should be appropriate to the risk significance scores and tie in with your action plan* • *Put review dates in your local calendar/s, e.g. Microsoft Outlook tasks or equivalent systems* • *If there is a significant change in your workplace, remember to check your risk assessment and, where necessary, amend it*

Appendix 2: Risk Matrix

Table 1 – CONSEQUENCE SCORE

Type of Risk	Insignificant - 1	Minor - 2	Moderate - 3	Severe - 4	Catastrophic - 5
Business Continuity	Loss/interruption of critical service or facility 1-8 hours Loss/interruption of non-critical service or facility >1 day Short term low staffing level temporarily reduces service quality (< 1 day)	Loss/interruption of critical service or facility 8 hours – 1day Loss/interruption of non-critical service or facility >1 week Ongoing low staffing level reduces service quality	Loss/interruption of critical service or facility >1 day Permanent loss of non-critical service or facility Unsafe staffing level or competence (>1 day)	Loss/interruption of critical service or facility >1 week Unsafe staffing level or competence (>5 days) Loss of key staff	Permanent loss of critical service or facility Loss of several key staff. Ongoing unsafe staffing levels or competence
Complaint	Very low level complaint. Likely to be diffused without the need for escalation.	Low level complaint. Resolved locally by the appropriate manager. (e.g. Pt waited longer in clinic than expected, minor issues with care/treatment)	Moderate complaint usually highlighting a number of related issues around care, treatment or administrative failings. (e.g. Poor general care/treatment, delays with referrals for treatment, poor attitude, poor handling of admission/discharge /transfer)	Serious complaint potentially resulting in claim and/or an adverse impact on the Trust's reputation. (e.g. Patient suffers massive life changing impact as a direct result of poor care/treatment) Ombudsman investigation likely to be upheld.	Very serious complaint likely to result in significant claim and/or a major adverse impact on the Trust's reputation. (e.g. patient died as a direct result of poor care/treatment) Ombudsman investigation likely to be upheld.
Financial	Loss/overspend of £100,000 or less Risk of claims remote	Loss/Overspend > £100,000 but no more than £500,000 Claim < £100,000	Loss/Overspend > £500,000 but no more than £1,000,000 Claim(s) between £100,000 and £1,000,000	Loss/Overspend > £1,000,000 but no more than £5,000,000 Claims between £1.000,000 and £5 million	Overspend/Loss of > £5m Loss of contract/payment by results Claim(s) >£5 million
Compliance & Regulatory	No or minimal impact or breach of guidance/statutory duty	Single failure to meet internal standards Reduced performance rating if unresolved	Repeated failure to meet internal standards Challenging external recommendations/improvement notice	Non-compliance with national standards with significant risk to patients if unresolved. Low performance rating Critical report	Total unacceptable level of quality of treatment/service Inquest/Ombudsman inquiry Gross failure to meet national targets Zero performance rating Severely critical report
Health and Safety	Minimal injury requiring no/minimal	Minor injury or illness, first aid treatment needed	Moderate injury requiring professional	Major injuries, or long term incapacity/	Incident directly leading to death Multiple permanent

Type of Risk	Insignificant - 1	Minor - 2	Moderate - 3	Severe - 4	Catastrophic - 5
	intervention or treatment. No time off work No or minimal impact or breach of guidance/statutory duty Minimal or no impact on the environment	Requiring time off work <7 days Breach of statutory legislation (no harm caused) Minor impact on environment	intervention RIDDOR reportable, requiring time off work for 7-14 days Single breach in statutory legislation (harm caused) Challenging external recommendations/improvement notice Moderate impact on environment	disability Requiring time off work for >14 days Enforcement action Multiple breaches in statutory legislation (harm caused) Improvement notices Major impact on environment	injuries or irreversible health effects Prosecution Complete systems change required Catastrophic impact on environment
Infection Control	Failure of laboratory diagnostic test for one day delaying results eg *Clostridium difficile* ELISA run. Sporadic alert organism cases. Media interest unlikely	Clusters of cases of an alert organism resulting in further investigation Temporary breakdown in communication link between IT systems e.g. Telepath and PICS	Cluster or outbreak affecting small numbers of patients and triggering escalation plan. E.g. Norovirus outbreak, period of increased incidence of *Clostridium difficile*. Local media coverage possible	Decontamination failure resulting in restriction of services Breach of mandatory infection control targets Downgrading by care quality commission Local media coverage likely	Serious breach in compliance with infection control procedures resulting in major incident such as hospital-acquired Legionella outbreak. National media coverage likely
Information Governance	Potential or minor breach of confidentiality or non-person identifiable data. Only a single individual affected Media interest very unlikely	Potentially serious breach of confidentiality, or data loss. Between 2 and 20 people affected. Possible media interest	Serious breach of confidentiality, or loss of personal data. Between 21 and 100 people affected. Low key local media coverage	Serious breach of confidentiality, or loss of data. Between 100 - 1000 people affected, or information is particularly sensitivity e.g. sexual health details, Local media coverage	Serious breach of confidentiality or data loss, over 1000 people affected, potential for identity theft. National media coverage
Operational	Minor schedule slippage – no effect on achievability of objectives Short term low staffing level temporarily reduces service quality (< 1 day)	Significant schedule slippage but no other effect on achievability of objectives Ongoing low staffing level reduces service quality	Some non-key objectives not achievable Late delivery of key objective / service due to lack of staff Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objectives Uncertain delivery of key objective / service due to lack of staff. Loss of key staff Very low staff morale No staff attending mandatory/key training	Non delivery of key objectives/ Substantial failure to meet specification Non delivery of key objective / service due to lack of staff. Ongoing unsafe staffing levels or competence No staff attending mandatory/key training on an ongoing basis

Type of Risk	Insignificant - 1	Minor - 2	Moderate - 3	Severe - 4	Catastrophic - 5
Patient Safety (Clinical)	Minimal injury requiring no/minimal intervention or treatment. Peripheral element of treatment or service sub optimal	Minor injury or illness that required extra observations or minor treatment and caused minimal harm to one or more patients. Overall treatment or service suboptimal Minor implications for patient safety.	Moderate injury which resulted in moderate increase in treatment and that caused significant but not permanent harm Treatment or service has significantly reduced effectiveness Major patient safety implications if findings are not acted on	Major injuries, or long term incapacity/ disability Permanent harm to one or more patients Mismanagement of patient care with long term effects	Incident directly leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Reputation	Rumours Potential for public concern	Local media coverage – short term reduction in public confidence Elements of public expectation not being met	Local media coverage – long term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation (questions in The House) Total loss of public confidence

TABLE 2 - LIKELIHOOD SCORE

Descriptor	Rare - 1	Unlikely - 2	Possible - 3	Likely - 4	Highly Likely - 5
Frequency	May not occur for several years (i.e. more than 5)	Could occur at least once in a 5 year period	Could occur at least once a year	Could occur at least once in 6 months	Could occur at least once per month
Probability	<1%	1% - 5%	5% - 45%	45% - 85%	> 85%
	Will only occur in exceptional circumstances	Unlikely to occur	Reasonable chance of occurring	Likely to occur	More likely to occur than not

TABLE 3 – RISK RATING

Likelihood	Consequence				
	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Highly Likely 5	Low 5	Moderate 10	Significant 15	High 20	High 25
Likely 4	Low 4	Moderate 8	Significant 12	High 16	High 20
Possible 3	Low 3	Moderate 6	Moderate 9	Significant 12	Significant 15
Unlikely 2	Low 2	Low 4	Moderate 6	Moderate 8	Moderate 10
Rare 1	Low 1	Low 2	Low 3	Low 4	Low 5
Black line = Trust tolerance level					