Essex Partnership University
NHS Foundation Trust

Data Protection (Privacy) Impact Assessment (DPIA) Form

The Essex Partnership University NHS Foundation Trust's (EPUT) data processing activity MUST comply with the (UK) General Data Protection Regulation/Data Protection Act (2018).

This (Stage 1) Section of the Data Protection Impact Assessment will provide guidance for evaluating whether a full scale DPIA should be conducted. This form will assist Information Asset Owners in identifying how the collection of people's personal information may affect their privacy.

In this evaluation process you are required to answer the following set of screening questions relating to the key characteristics of the project and the system that the project will deliver. Answers to the questions need to be considered as a whole, in order to determine whether the overall impact and related risk warrant a full scale DPIA (Stage 2).

***DPIA Ref Number:**	
Name of Project:	
Proposed Implementation Date:	
Name of Person Completing DPIA:	
Contact Details:	
Date of Completion:	

**This will be entered by the IG Team*

If you have any questions or would like any help in completing this document please contact the IG Team at [redacted]

Stage 1 – Screening Questions

Screening Question	Response (Yes/No)	Rationale
Will the project involve the collection of new information about data subjects?	☐ Yes ☐ No	
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☐ Yes ☐ No	

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 ☐ No	
Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☐ Yes ☐ No	
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 particularly private.	☐ Yes ☐ No	
Does the project involve you using new technology which might be perceived as being privacy intrusive i.e. the use of cookies (a software application) to download personal information whilst using the software / mobile devices to record conversations?	☐ Yes ☐ No	
Has consent been gained from the individual and appropriately recorded for future reference?	☐ Yes ☐ No	
Is it essential the data remains identifiable?	☐ Yes ☐ No	
Will the data be used for research?	☐ Yes ☐ No	

If you have answered "Yes" to any of the above please continue on to Stage 2. If you have answered "No" to all of the above questions then please sign the Sign-off and Approval page and send to the IG team.

Stage 2 – Full Data Privacy Impact Assessment

This stage should be completed if you answered "Yes" to any of the questions above or if it is clear that a Full DPIA is required from the outset.

2.1 Project Aim & Objective? The project scoping document can be used here, it is a good idea to link/ embed the document. You should explain the project objectives/purpose, benefits to organisation, and any other parties, such as the data subjects (those individuals who you will be collecting information about). You should be able to summarise the reason for the DPIA here.

2.2 Information Flows/Processing of Information Any suggested collection, purpose and volume of Person Identifiable Information (PII) should be recorded here. If a Data Flow Mapping exercise has been completed this should be linked here and the information below should provide a summary of those maps:		
Whom is the Information processed about? (please tick ✓ all the related options)		**Employees**
		Patients
		Students
		Agency Staff/Volunteers
		Partner Businesses or Organisations

		Other	**Parent of Child plus details of any other proxy access granted by parent.**
What are the Data Classes that will be held or processed as part of the implementation or change? (please tick ✓ all the related options) (When data is processed,interpreted, organised, structured or presented so as to make them meaningful or useful, it is called information.)			**Person sensitive details** (name, address, postcode, date of birth, NHS number, Gender, GP Practice, Consultant, Third Party Relationships, Email Address, IP address – *please delete as appropriate*)
			Family, lifestyle and social circumstances (marital status, housing, travel, leisure activities, membership of charities – *please delete as appropriate*)
			Education and training details (qualifications or certifications, training records)
			Employment details (career history, recruitment and termination details, attendance details, appraisals, other – *please delete as appropriate*)
			Financial details (income, salary, assets, investments, payments, other – *please delete as appropriate*)
			Criminal proceedings, outcomes and sentences
			Goods or services (contracts, licenses, agreements etc.)
			Goods or services (contracts, licenses, agreements etc.)
			Religious or other beliefs of a similar nature
			Political opinions

		Physical or mental health conditions	
		Offences including alleged offences	
		Sexual health	
		Trade Union membership	
		Other	Include additional events on page 10.
How will the information be collected and transferred to the organisation?			
Who will have access the information?			
Where will the information be held?	☐ On paper ☐ On a database saved on a network folder/drive ☐ External Website / system ☐ On a dedicated system saved to NHS network ☐ Other – please state below:		
What will the information be used for?			
What are the retention periods for this data? (please refer to the NHS Code of Practice Records Management) How will it be destroyed/deleted?			

Will the Information be shared with anyone else? If so Who?	☐ Yes ☐ No Please provide details:
Does this Project/ Initiative involve the use of a System Supplier? If so please provide details.	☐ Yes ☐ No Please provide details:
How will the data be kept up to date and checked for accuracy and completeness?	
Will any data be transferred outside the organisation premises or systems	☐ Yes ☐ No Please provide details: ☐ Yes –Within the European Economic Area (EEA) ☐ Yes –Outside the European Economic Area (international) Please name the country:
Does this include back-up or server arrangements?	☐ Yes ☐ No Please provide details:
Is there a contingency plan / backup policy in place to manage the effect of an unforeseen event?	☐ Yes ☐ No Please provide details:
If personal, sensitive or business sensitive data is being processed by the system, has this been added to the relevant Data Flow Mapping document?	☐ Yes ☐ No Please provide details:

Attach Data Flow Mapping Spreadsheet here if you have completed this	

2.0 Legal Basis (see Appendix 1 for detail)	
2.1 What is the lawful basis for processing Personal Data under General Data Protection Regulation. DPA 2018 **NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care**	☐ 6) (1) a) Consent - (all article 7 conditions must be met ☐ 6) (1) b) Delivery of a Contract ☐ 6) (1) c) Legal Obligation ☐ 6) (1) d) Vital interests ☐ 6) (1) e) A public / official function / Interest
2.2 Does the processing involve special categories of data A) racial or ethnic origin of the individual B) the political opinions of the individual C) the religious or philosophical beliefs of the individual D) whether the individual is a member of a trade union E) processing of genetic or biometric data for uniquely identifying an individual F) physical or mental health of the individual G) sex life or sexual orientation of the individual	☐ Yes ☐ No Please provide details:
2.3 If Yes What is the lawful basis for processing Personal Data under General Data Protection Regulation Article 9.	☐ 9) (2) a) Consent – (all article 7 conditions must be met) ☐ 9) (2) b) Employment, social security etc. ☐ 9) (2) c) Vital interests ☐ 9) (2) d) Legitimate activities (not to be used for public authorities)

NB –DO NOT select 6) (1) a) if processing is for the purpose of direct health or social care	☐ 9) (2) e) Data already been made public by subject ☐ 9) (2) f) Legal obligation ☐ 9) (2) g) Public interest ☐ 9) (2) h) Provision of Health or Social Care ☐ 9) (2) i) Public health ☐ 9) (2) j) Historical or scientific research
2.4 Where consent is applied, Please provide details of the consent process and embed any consent forms **Note: Consent must follow Article 7 requirements**	☐ Explicit consent Provide details below:
2.5 Please indicate other legislation which provides a legal basis for processing **(Please tick relevant legislation or add details as necessary)**	☐ Children Act 1989 as amended 2004 ☐ Mental Capacity Act 2005 ☐ Health & Social Care Act 2012 ☐ Care Act 2014 ☑ H&SC (Safety and Quality) Act 2015 ☐ NHS Act 2006 ☐ Human Rights Act 1998 ☐ Data Protection Act 2018 Sch 1 para 2 ☐ Other (Please specify)

3.0 Risk Assessment (see Appendix 2 for examples)

	Consequence				
Likelihood	1 Negligible	2 Low	3 Medium	4 High	5 Extreme
1 Rare	L1	L2	L3	M4	M5
2 Unlikely	L2	L4	M6	M8	S10
3 Possible	L3	M6	M9	S12	H15
4 Likely	L4	M8	S12	H16	H20
5 Almost Certain	M5	M10	S15	H20	H25

3.1 Highlight Risks and Identify Controls

All key risks should be highlighted here with any controls that have been identified. All risks to the project should be held on a formal risk register

No	Summary of Risk	Risk to Individuals	Risk to the organisation	Compliance Risk	Identified Risk L/M/S/H	Proposed Controls	Residual Risk L/M/S/H
1							
2							
3							

* IG Team Use Only

DPIA Reviewed by:		Review Date:	
DPIA reviewed by Data Protection Officer for Approval	☐ Yes ☐ No Comment:		
DPIA reviewed by Cyber :	☐ Yes ☐ No Comment:		
Does the Trust have a compliant Privacy Notice for this process	☐ Yes ☐ No Comment:		

Stage 1 Agreed	☐ Yes ☐ No
Stage 2 Required	☐ Yes ☐ No Comment:

Sign Off and Approval – Stage 1

Once this document has been completed and the solutions agreed it should be signed off by the DPO, Project Lead and the Information Governance Manager within the organisation

	Name	Date	Signed
Project Lead			
Information Governance Manager			

Sign Off and Approval – Stage 2

Once this document has been completed and the solutions agreed it should be signed off by the DPO and SIRO within the organisation

	Name	Date	Signed
SIRO	Trevor Smith		
Data Protection Officer	Claire Sladden		

Appendix 1 – Glossary of Terms

Item	Definition
Personal Data	This means data which relates to a living individual (data subject) who can be identified, directly or indirectly, by reference to an identifier such as name, an identification number, location data, and online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person: A) from those data, or B) from those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller. It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual
Special Categories of Data	This means personal data consisting of information as to the: H) racial or ethnic origin of the individual I) the political opinions of the individual J) the religious or philosophical beliefs of the individual K) whether the individual is a member of a trade union L) processing of genetic or biometric data for uniquely identifying an individual M) physical or mental health of the individual N) sex life or sexual orientation of the individual
Direct Marketing	This is "junk mail" which is directed to particular individuals. The mail which are addressed to "the occupier" is not directed to an individual and is therefore not direct marketing. Direct marketing also includes all other means by which an individual may be contacted directly such as emails and text messages which you have asked to be sent to you. Direct marketing does not just refer to selling products or services to individuals, it also includes promoting particular views or campaigns such as those of a political party or charity.
Automated Decision Making	Automated decisions only arise if 2 requirements are met. First, the decision has to be taken using personal information solely by automatic means including profiling, which produces legal effects concerning the data subject or similarly affects them. For example, if an individual applies for a personal loan online, the website uses algorithms and auto credit searching to provide an immediate yes / no decision. The second

	requirement is that the decision has to have a significant effect on the individual concerned.
International organisation	Means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Information Assets	Information assets are records, information of any kind, data of any kind and any format which we use to support our roles and responsibilities. Examples of Information Assets are databases, systems, manual and electronic records, archived data, libraries, operations and support procedures, manual and training materials, contracts and agreements, business continuity plans, software and hardware.
SIRO (Senior Information Risk Owner)	This person is an executive who takes ownership of the organisation's information risk policy and acts as advocate for information risk on the Board
IAO (Information Asset Owner)	These are senior individuals involved in running the relevant service/department. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. They are responsible for providing regular reports regarding information risks and incidents pertaining to the assets under their control/area.
IAA (Information Asset Administrator)	There are individuals who ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date. These roles tend to be system managers
Explicit Consent	Express or explicit consent is given by the data subject freely given, specific, informed and unambiguous indication of the data subjects wishes, usually orally (which must be documented in the patient's casenotes) or in writing, to a particular use of disclosure of information.
Anonymity	Information may be used more freely if the subject of the information is not identifiable in any way – this is anonymised data. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow individuals to be identified. A combination of items increases the chances of patient identification. When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek

	consent, general information about when anonymised data will be used should be made available to patients.
Pseudonymisation	Means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person Patient identifiers such as name, address, date of birth are substituted with a pseudonym, code or other unique reference so that the data will only be identifiable to those who have the code or reference.
Information Risk	An identified risk to any information asset that the Trust holds. Please see the Information Risk Policy for further information.
Privacy Invasive Technologies	Examples of such technologies include, but are not limited to, smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining and logging of electronic traffic. Technologies that are inherently intrusive, new and sound threatening are a concern and hence represent a risk
Authentication Requirements	An identifier enables organisations to collate data about an individual. There are increasingly onerous registration processes and document production requirements imposed to ensure the correct person can have, for example, the correct access to a system or have a smartcard. These are warning signs of potential privacy risks.
Retention Periods	Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time. If an organisation decides that it needs to keep records longer than the recommended minimum period, it can vary the period accordingly and record the decision and the reasons behind. The retention period should be calculated from the beginning of the year after the last date on the record. Any decision to keep records longer than 30 years must obtain approval from The National Archives.
Information Governance Alliance (IGA) Records	Is a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice. The

Management NHS Code of Practice	code of practice contains an annex with a health records retention schedule and a Business and Corporate (non-health) records retention schedule.
(UK) General Data Protection Regulation (EU) 2016/679 (GDPR)	European legislation (applied in UK law by the Data Protection Act 2018) on the protection of natural persons with regard to the processing of personal data. The Regulation defines the ways in which information about living people may be legally used and handled. The 6 principles of the Regulation state the fundamental principles relating to processing personal data must: • Be processed fairly and lawfully. • Collected for specified, explicit and legitimate purposes • Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. • Be accurate and, where necessary, kept up to date. • 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. • 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. The Regulation also requires that the Data Controller and Data Processor are both able to demonstrate compliance with these principles.
Privacy and Electronic Communications Regulations 2003	These regulations apply to sending unsolicited marketing messages electronically such as telephone, fax, email and text. Unsolicited marketing material should only be sent if the requester has opted in to receive this information.
Article 6 Conditions of Processing	1) (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes - only lawful if ALL article 7 conditions for consent are met 1) (b) A contract with the individual: for example, to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract. 1) (c) Compliance with a legal obligation: if you are required by UK or EU law to process the data for a particular purpose, you can. 1) (d) Vital interests: you can process personal data if it is necessary to protect someone's life. This could be the life of the data subject or someone else.

	1) (e) A public task: if you need to process personal data to carry out your official functions or a task in the public interest – and you have a legal basis for the processing under UK law – you can. If you are a UK public authority, our view is that this is likely to give you a lawful basis for many if not all of your activities. 1) (f) Legitimate Interest: If you need to process personal data in the legitimate interests of the Data Controller or 3rd Party or Data Subjects Rights in particular where data subject is a child. NB 1) (f) does not apply to processing carried out by Public authorities in the performance of their tasks.
Article 9 Conditions of Processing special categories of data	(1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. (2) Paragraph 1 shall not apply if one of the following applies: 2) (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject only lawful if ALL article 7 conditions for consent are met (see column D)" 2) (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; 2) (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; 2) (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact

	with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; 2) (e) processing relates to personal data which are manifestly made public by the data subject; 2) (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; 2) (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; 2) (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; 2) (i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 2) (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
Article 7 (Recital 32) Conditions for Consent	Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website,

	choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

Appendix 2 – Examples of Risk

EXAMPLES OF PRIVACY AND RELATED RISKS
RISKS TO INDIVIDUALS
Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
New surveillance methods may be an unjustified intrusion on their privacy.
Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
The sharing and merging of datasets can allow organisations to collect a much wider set of information that individuals may expect.
Identifiers might be collected and linked, which prevents people from using a service anonymously.
Vulnerable people may be particularly concerned about the risks of identification of the disclosure of information.
Collecting information and linking identifiers may mean that an organisation is no longer using information which is safely anonymised.
Information, which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, presents a greater security risk.
If a retention period is not established, information might be used for longer than is necessary.
CORPORATE RISKS
Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
Problems, which are only identified after the project has launched, are more likely to require expensive fines.
The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engagement with the organisation.
Information, which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, is less useful to the business.

Public distrust about how information is used can damage an organisations reputation and lead to loss of business.
Data losses (which damage individuals) could lead to claims for compensation.
COMPLIANCE RISKS
Non-compliance with the DPA.
Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
Non-compliance with sector specific legislation or standards
Non-compliance with Human Rights legislation