Best Care
Healthy Communities

NHS
Birmingham
Community Healthcare
NHS Foundation Trust

Data Protection Impact Assessment

This document must be completed for any new project/initiative/process or change in current process within the Trust which will involve processing of data which is likely to result in a high risk to rights and freedoms of individuals. This form should be completed prior to the processing of any data.

Data Protection Impact Assessments are a mandatory requirement under the Regulation (EU) 2016/679 (General Data Protection Regulation) and of the Information Governance Toolkit. These assessments are designed to ensure that security and confidentiality of personal identifiable data is maintained during any new process or change in process and that appropriate controls are in place.

Requirements as set out in Regulation (EU) 2016/679 (General Data Protection Regulation) are incorporated within the questions included below.

Please complete the following sections in as much detail as possible and contact the Trust's Data Protection Officer for further guidance or assistance in completing the sections.

A. VERSION CONTROL (MASTER DPIA TEMPLATE)

Document history:

Version number	**Author**	**Summary of change**	**Date**
1.0	Ben Pumphrey, Trust DPO	New Document (replacing Privacy Impact Assessment)	13.06.2018
1.1	Ben Pumphrey, Trust DPO	Updates to template – reformatting and inclusion of clearer guidance	09.09.2018
1.2	Ben Pumphrey, Trust DPO	Update to risk matrix guidance at Section I.	15.10.2019

B. VERSION CONTROL (THIS DATA PROTECTION IMPACT ASSSESSMENT)

Version number	**Author**	**Any changes? Summary of key changes**	**Date of review (and date of next planned review)**

C. SUMMARY OF DATA PROTECTION IMPACT ASSESSMENT

Complete right hand column – this section should contain a high level summary of your project and nature of personal data to be processed

a. Project name	
b. Project manager	
c. Information Asset Owner and contact details	
d. High level description of initiative / project	
e. Summary of personal data which will be involved	
f. How will the risks to the data subject be mitigated/managed?	
g. Are there any other organisations involved, and what are the governance arrangements in place with them?	
h. Frequency of review of DPIA *(article 35(11) GDPR).* Where an initiative is described as 'ongoing' or 'indefinite', review should ordinarily happen after year 1, thereafter every 3 years.	

D. DETAILED DATA PROTECTION IMPACT ASSESSMENT – A SYSTEMATIC DESCRIPTION OF THE PROCESSING PROPOSED

1. Describe here the context of the processing – what is the underlying issue that the data processing is designed to address?		GDPR article 35(7) and recital 90
2. What is/are the purpose(s) of the processing?	The purposes of processing personal data for this project are:	GDPR article 35(7) and recital 90
3. Could this project be undertaken (or the same outcome achieved) without using personal data – including through the use of an anonymised data-set? *See also section H below.*	Yes: [ ] No: [ ]	Article 10, 25 and 35(7)(b) GDPR
4. What is the scale and scope of the data processing being undertaken? Is the full scope covered by this DPIA? If not where else is it covered? ***This section may effectively summarise other elements of the data processing.***	*The total number of data subjects is likely to be .* *They are drawn from*	GDPR Article 35(3)(b) GDPR recital 90
5. What are the data flows? See also section E below.		
***6.* How is the processing undertaken?**		GDPR article 35(7)(a)
7. Is any automated processing or profiling of individuals being undertaken		GDPR Article 22 GDPR recital 90

8. Does the project involve new or inherently privacy invasive technologies?	Yes [ ] No [ ]	Article 35(1) GDPR
9. Where will the data be stored? Is any of this off-site or on (re)movable devices?		Article 32 GDPR
10. Are there any privacy enhancing technologies in place where data is at rest?		
11. How will data be transferred? **12. What secure arrangements are in palce for transfer/are there any privacy enhancing technologies in place where data is being transferred?**		Article 32 GDPR
13. What measures are in place to ensure that only adequate, relevant and necessary data processed for the project?		Article 5(1)(c) GDPR
14. Will the data be kept up to date – is the data being used a one-time extract from existing systems, or is it a live system? See also	[ ] Live system [ ] Single extract [ ] Updating extracts at [frequency]	Article 5(1)(d) GDPR
15. What is the duration of the project?		Article 5(1)(e) GDPR
16. What are the retention periods for this data and are these documented? **17. Will any data be destroyed before the project is over?** **18. What will happen to the data at the termination of the project?**	[ ] Storage [ ] Destruction	GDPR article 35(7)(a) and (d) and recital 90

E. ABOUT THE DATA BEING PROCESSED

19. Whose data is being processed? ***Tick all that apply***	[ ] Patient [ ] Staff [ ] Other *(specify):*	Article 35(7)(a) GDPR
20. What is the data being processed? ***WARNING: You should be able to justify why you need each kind of data in order to achieve or enhance the outcome.***	*Insert a description and / or complete the following list*: [ ] Name [ ] Address [ ] Postcode [ ] DoB [ ] NHS number [ ] PAS number [ ] GP [ ] Gender [ ] NI details [ ] Other identifiers:	Article 35(7)(a) GDPR
21. Is there any special category personal data being processed? ***WARNING: You should be able to justify why you need each kind of data in order to achieve or enhance the outcome. NB if you are sharing full records history of a patient all of these categories may be engaged.***	*Insert a description and / or complete the following list*: [ ] Information about health or disability [ ] Genetic and/or biometric details [ ] Racial or ethnic origin [ ] Political views [ ] Religious or philosophical beliefs [ ] Sex-life and/or sexual orientation [ ] Criminal history, offences, or convictions	Article 35(7)(a) GDPR
22. Are there any other sensitivities about the information being processed?	*Does it address, for instance, financial or immigration matters?*	Article 35(7)(a) GDPR
23. What is the source of the data?	[ ] Existing records applied to this activity *If existing records, does the project involve using that data in a way which would be contrary to the expectations of the data*	

	subject, or for a general purpose which is different to that which the data was originally obtained? [ ] A newly collected data-set for this activity / project *If a newly collected data set, from whom is the data collected – the patient/staff member concerned, other systems or external organisations?*	
24. Does the project/process involve new linkage of personal data with data in other collections, or significant changes in data linkages?	[ ] Yes [ ] No If yes, description of the linkages:	GDPR article 5(1)(b)
25. What checks, if any, have been made regarding the accuracy and relevance of the data in question?		GDPR Article 5(1)(c)

F. TRANSFER, DATA SHARING AND EXTERNAL INVOLVEMENT IN THE PROJECT

26. Will any data processors handle this data on behalf of the Trust?		Article 28 GDPR
27. Has due diligence been undertaken on the data processor?		
28. Is a data processing agreement in place with the contractor which discharges the requirements of Article 28 GDPR?		
29. What third parties are involved in this data processing activity?		Article 26 GDPR
30. If Trust data is transferred to a third party, what controls or		Article 26

restrictions (if any) are in place in terms of what happens to the data following transfer to the third party?		GDPR
31. Who is responsible for providing fair processing information to the data subjects?		Article 26 GDPR
32. Is an information sharing agreement or protocol to be entered into with the other party, where they are a Data Controller?	[ ] Yes *(embed a copy if so)* [ ] No	Article 26 GDPR

G. LEGAL COMPLIANCE AND GOVERNANCE

33. By reference to the legitimising conditions in Article 6 GDPR, what is the lawful basis for the purposes of GDPR for processing the data in question? **34. Please also insert a description of how the legal basis is justified – e.g. if consent is relied upon, how has it been obtained? If 'legal obligation' is relied upon, what is the source of the legal obligation?**	[ ] Explicit, unambiguous consent [ ] Contractual performance [ ] Legal obligation [ ] To protect vital interests [ ] To serve the public interest [ ] The exercise of the Trust's functions [ ] The service of legitimate interests of the person to whom the Trust intends to disclose the data in question.	
35. By reference to the legitimising conditions in Article 9 GDP (read with the Data Protection Act 2018), what is the lawful basis for the purposes of GDPR for processing any special category personal data?		
36. By reference to common law confidentiality concepts, what is the lawful basis for processing personal data, if any?	[ ] Implied consent / within the reasonable expectations of the data subject / no misuse [ ] Explicit consent [ ] Statutory authorisation / obligation to share	Article 5(1) GDPR

	[ ] Public interest [ ] s. 251 authorisation	
37. Are there any Human Rights Act implications for processing the data in question?	[ ] Yes [ ] No *Insert further details as appropriate:*	Article 5(1) GDPR
38. Where the project is research, has REC approval been given for the project?	[ ] Yes [ ] No [ ] Not applicable	
39. What Codes of Practice or other guidance has been considered in connection with this data processing activity?		Article 35(8) GDPR
40. Have any other data protection impact assessments been undertaken in connection with similar projects, whether by the Trust or others?		Article 35(10) GDPR
41. Has advice been sought on whether there are any other legal considerations affected by this project, and if so what are they and how have they been addressed?		

H. THE PROPORTIONALITY AND NECESSITY OF PROCESSING

42. What are the potential benefits to data subjects of undertaking the processing? Are these at the individual/specific level, or generally for all Trust staff/service users, etc.		Article 35(7)(b) GDPR
43. What are the potential benefits to the Trust of undertaking this processing?		Article 35(7)(b) GDPR

44. What are the potential benefits to any third parties of undertaking this processing?		Article 35(7)(b) GDPR
45. Could the same benefits be achieved without processing personal data (or by processing less personal data), and if so to what degree?		Article 35(7)(b) GDPR

I. RISKS TO DATA SUBJECTS, MITIGATIONS AND MANAGEMENT OF RISK

From the perspective of the data subject, what are the risks to data subjects associated with this processing? ***(GDPR article 35(7)(c), recitals 84 and 90)***

Risk 1: Illegitimate Access

Details	**Description of risk**	**Mitigations/measures in place to address risk**
Source of risk		
Nature of risk		
Likelihood of risk materialising (1-5 + narrative justification)		
Severity of risk if it materialises (1-5 + narrative justification)		
Overall risk score (Likelihood x Severity)		

Risk 2: Undesired Modification

Details	Description of risk	Mitigations/measures in place to address risk
Source of risk		
Nature of risk		
Likelihood of risk materialising (1-5 + narrative justification)		
Severity of risk if it materialises (1-5 + narrative justification)		
Overall risk score (Likelihood x Severity)		

Risk 3: Loss or disappearance of data

Details	Description of risk	Mitigations/measures in place to address risk
Source of risk		
Nature of risk		
Likelihood of risk materialising (1-5 + narrative justification)		
Severity of risk if it materialises (1-5 + narrative		

justification)		
Overall risk score (Likelihood x Severity)		

Risk 4: Other ([insert details]; *repeat as necessary for any further risks identified*)

Details	**Description of risk**	**Mitigations/measures in place to address risk**
Source of risk		
Nature of risk		
Likelihood of risk materialising (1-5 + narrative justification)		
Severity of risk if it materialises (1-5 + narrative justification)		
Overall risk score (Likelihood x Severity)		

J. PROTECTION OF DATA SUBJECTS' RIGHTS

46. Is the data processing here likely to go beyond the expectations of data subjects in terms of how their data will be handled by data subjects, or could it cause distress or damage to data subjects? *(See*		Article 35(7)(b) GDPR and Articles 12-23 GDPR

also section I above)		
47. Does this project / process involve new or changed data access or disclosure arrangements that may be unclear? How are these being addressed?		Articles 12-14 GDPR
48. How will data subjects be informed of all the processing and disclosures associated with this processing activity?		Articles 12-14 GDPR
49. Data subjects have a number of further rights in connection with their personal data, including the right of access and the right to object to data processing. Is it envisaged that these rights would be curtailed in connection with this data processing?		Articles 15-23 GDPR
50. Do the systems in place support data subject rights or choices to opt out/not to participate?		
51. What procedures can be put in place for the rectifying, blocking, erasure and destruction of the data following an individual request or court order?		
52. Are any international transfers of data envisaged? **53. If so, to where?** **54. Are data subjects aware of this?** **55. How is the data transfer made lawful by reference to Article 45-47 GDPR?**		

K. INVOLVEMENT OF INTERESTED PARTIES WHEN UNDERTAKING THIS ASSESSMENT *(Article 35(9) GDPR, Article 36 GDPR)*

56. Have data subjects been involved in this assessment, and if so how? What was the output from their involvement?		Article 35(9) GDPR)
57. Has the Trust's data protection officer been involved in this assessment, and if so how? What was the output from their involvement?		Article 35(2) GDPR
58. Has the Trust's Caldicott Guardian and/or SIRO been involved in this assessment?		
59. Has the Information Commissioner been consulted about the project?		Article 36 GDPR
60. Have any other parties been involved in undertaking this assessment?		

L. OVERALL ASSESSMENT OF RISK FROM THIS PROJECT

<table>
<tr>
<td>61. Overall conclusions around the risks, benefits and any other impacts on data subjects from this processing activity</td>
<td></td>
<td>Article 35(1) GDPR</td>
</tr>
<tr>
<td>62. Confirmation that, in light of the risks and notwithstanding any mitigations put in place, it is appropriate to continue to proceed to process the data in question</td>
<td>
<table>
<tr><td>Details</td><td>Date</td></tr>
<tr><td>[Information Asset Owner]</td><td></td></tr>
<tr><td>[Data Protection Officer]</td><td></td></tr>
<tr><td>[Caldicott Guardian (if necessary)]</td><td></td></tr>
</table>
</td>
<td>Article 35(1) GDPR</td>
</tr>
</table>