A lifetime of specialist care

Royal Brompton & Harefield NHS
NHS Foundation Trust

Data Protection Impact Assessment (DPIA)

(A) Preliminary Questions

1	Date	**29/04/19**
2	Title and Description of the application/project	**Datix upgrade – upgrading the current system to Datix CloudIQ**
3	Name of the Information Asset Owner of the application/project	**[name redacted], Quality & Safety** **[name redacted], IT & Informatics**
4	Does the application/project process personal data?	**Yes**
	If yes, for what purpose?	**The data is processed in line with the requirements of clinical governance; incidents, complaints, mortality, claims, etc.**

(B) Trigger Questions

		Yes	No
1	Does the processing operation involve evaluation or scoring?	✓	
2	Does the processing operation allow automated decisions producing legal or similar significant effects on data subjects?		✓
3	Does the processing operation involve systematic monitoring?	✓	
4	Are special categories of personal data processed?	✓	
5	Is the processing operation on a large scale?	✓	
6	Have datasets been matched or combined?	✓	
7	Does the processing operation involve data concerning vulnerable data subjects?	✓	
8	Does the processing operation involve new technological or organisational solutions?	✓	
9	Does the processing operation prevent data subjects from exercising a right or using a service or a contract?		✓

If you have replied YES to at least two of the above questions, proceed with the DPIA. If not, then a DPIA is not needed.

Impact Assessment

1	**What type of data are being processed?**	Personal Data	✓
		Special Categories of personal data	✓
		Other	✓

2	**Which are the recipients of personal data?**	Joint Data Controllers	✓
		Data Processors	✓
		Authorised Persons	✓

3	Indicate the period for which the personal data are stored and the reasons for determining set period, or if that is not possible the criteria used to determine that period.	The information will be kept indefinitely (or until the contact expires) and will be stored on a server hosted by Datix. The length of time the data is to be stored is in line with the requirements set out by clinical governance.
4	Indicate the assets through which the application/project processes personal data.	Hardware
		Software
		By automated means
5	Does the application/project process data in compliance with an ICO approved GDPR code of conduct, (Art 40 GDPR e.g. Codes of conduct and certification)?	Yes

6	Are the purposes for which the data will be processed specified, explicit and legitimate?	Yes ✓	No
	List the purposes:		
7	Has the legal basis for the processing been identified?	Yes ✓	No
	List the legal bases:		

	The legal gateway to undertake the using special categories of information for this purpose under GDPR is Article 9(2)(h), that the: 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 […]. For this to be achieved, however, one of the gateways from Article 6 will also need to have been satisfied. The most appropriate is 6(1)(e), that: For direct patient care, consent not required		
8	Is the processing adequate, relevant and limited to what is necessary (data minimisation)?	Yes ✓	No
	How have we considered minimising data? Only essential information is to be automatically pulled from PAS – this will only be in the case of an incident, complaint claim, mortality review, etc., related patients. Depending on what the request is (i.e incident) certain information of importance to that request will be pulled (i.e. incident related to patient would utilise name, dob and hospital number. However, if it is a complaint then the patient's name and address would be utilised).		
9	Has adequate notice been provided to data subjects (patients or staff)?	Yes ✓	No

Are data subject's rights respected?

		Yes	No	Maybe
	Right of access	✓		
	Right to data portability	✓		
	Right to rectification	✓		
	Right to erasure	✓		
	Right to restriction	✓		

International Transfers

Which are the conditions for transfer to third countries or international organisations?	Data are not transferred	✓
	Standard Model Clauses/other binding agreements	
	Adequacy Decision	
	Binding Corporate Rules	
	Other Derogations	

Risk Assessment

The following analysis takes into account the risk that the application/project may cause to the rights and freedoms of the data subjects. For each risk, the impact and likelihood of occurrence shall be indicated.

Impact: 1 – Negligible; 2 – Minor; 3 – Moderate; 4 – Major; 5 - Catastrophic

Likelihood: 1 – Rare; 2 – Unlikely; 3 – Possible; 4 – Likely; 5 – Almost Certain

Result: Multiplication of 'impact' and 'likelihood'

	Risk	**Impact**	**Likelihood**	**Result**
1	Discrimination	**2**	**2**	**4**
2	Identity theft or misuse	**2**	**2**	**4**
3	Financial loss	**1**	**1**	**1**
4	Loss of reputation	**1**	**1**	**1**
5	Loss of confidentiality of personal data (in particular if protected by professional secrecy)	**2**	**3**	**6**
6	Loss of data (i.e. ransomware, zero-day attacks)	**3**	**4**	**12**
7	Unauthorised deciphering or compromised algorithm	**2**	**2**	**4**
8	Other significant social or economic damages	**1**	**1**	**1**
9	Loss of freedoms or rights	**1**	**1**	**1**

10	Impossibility of exercising control over data	**1**	**1**	**1**
11	Illegal access to special categories of personal data or security measures to protect that personal data	**1**	**1**	**1**
12	Profiling mechanisms unclear or update without communication to the data subject	**2**	**2**	**4**
13	Processing of data related to vulnerable persons (i.e. patients, workers, minors)	**3**	**4**	**12**
14	Large scale processing	**2**	**2**	**4**

Select each result of 8 or higher, identify security and/or organisation measures to reduce the risk and report the new result based on the application of such measures. If the NEW RESULT is still 8 or higher you will require prior consultation with the Information Governance team.

	Risk	**Measure to reduce the risk**	**New Result**	**Requiring prior consultation?**
6	Loss of Data	IT (onsite/Datix) carry out regular backups, and [security details redacted]		
13	Processing of data related to vulnerable persons (i.e. patients, workers, minors)	Incidents/claims/complaints etc., are reviewed once they have been logged on to the Datix system – by Q&S Leads, service leads etc		