Privacy Impact Assessment
Data Protection Act Compliance Check

Privacy Impact Assessment Data Protection Act Compliance Check for New or Changed Systems or Processes

Where the proposed new system or process is to use personal or sensitive data or significantly change the way in which personal data is handled, this compliance check must be completed as part of the PIA process.

Please be aware that a PIA also needs to be completed if there is a significant change to an existing system or process.

It must be completed as soon as this is identified by the Project Manager/System Manager or Information Asset Owner during the Business Case phase of the project. The Information Asset Owner must be informed as soon as possible as an Information Risk Assessment needs to be completed. This compliance check contributes to this assessment.

This process is a mandated requirement on the Information Governance Toolkit. Some of the considerations that will be taken into account are whether a new system/process will:

- Allow personal information to be checked for relevancy, accuracy and validity
- Incorporate a procedure to ensure that personal information is disposed of through archiving or destruction when it is no longer required
- Have an adequate level of security to ensure that personal information is protected from unlawful or unauthorised access and from accidental loss, destruction of damage
- Enable the timely location and retrieval of personal information to meet subject access requests

The Information Commissioner has designed the Privacy Impact Assessment Handbook. This can be found on the Information Commissioner's website www.ico.gov.uk. This gives full details about why and how to conduct a full scale, small scale, data protection and privacy check impact assessment.

How to complete

Please read through all the questions thoroughly and answer with as much detail as possible. If you require any assistance, please contact the Head of Information Governance.

Data Protection Act Compliance Check Template

I BASIC INFORMATION – New or existing Project, System, Technology or Legislation

1. Organisation and Project

Organisation	
Department	**Medical Division**
Project Name	**Telestroke**
New or Existing?	NewX ☐ Existing ☐

2. Contact Position and/or Name, Telephone Number and Email Address.

(This should be the name of the individual most qualified to respond to questions regarding the PIA)

Name	
Title	
Department	**Medical Division**
Phone Number	
E-Mail	

3. Description of the Program / System / Technology /Legislation (Initiative) being assessed.	Telestroke – development of a managed network solution (within N3 the NHS national secure network) which will enable 8 hospitals in 6 trusts to share expert Stroke Physician opinion for patients with suspected Acute conditions out of hours. This incorporates access to existing Trust Picture Archive and Communication Systems (PACS) supplemented by a database and a new service to provide end to end image and data connection.

4. Purpose/Objectives of the initiative (if statutory, provide citation).	Improve patient care and clinical outcomes by supporting quicker diagnosis and appropriate treatment

5. What are the potential privacy impacts of this proposal?	As per initial assessment – CT images will be available to Consultants at home via secure remote link and there will be an underpinning database for clinical audit and quality assurance processes. A patient's care episode may involve processing by way of access to images and data on the part of the Consultant on call working in another Trust

6. Provide details of any previous PIA or other form of personal data* assessment done on this initiative (in whole or in part).	n/a

IF THERE IS NO PERSONAL DATA INVOLVED, GO TO III DPA COMPLIANCE – CONCLUSIONS

***IMPORTANT NOTE: 'Personal data' means data which relate to a living individual who can be identified:**

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and 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.

(Data Protection Act, section 1)

II DATA PROTECTION PRINCIPLES (DPPs)

1 Principle 1: Fair and Lawful Processing

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 19-35

1.1 Preliminary

1.1.1 What type of personal data are you processing?	Images of patients (CT) Personal Identifiers of patients and participating Stroke Consultants
Please give examples of any sensitive personal data that you are processing.	The images form part of the record of patient treatment Clinical advice and details of patient experience form part of the audit dataset
1.1.2 Are sensitive personal data being differentiated from other forms of personal data?	Yes ☐ No X ☐
If yes, please specify procedures. If no, please indicate why not.	All processing within system is in accordance with schedules 2 and 3

1.2 Schedule 2 - Grounds for Legitimate Processing of Any Personal Data

1.2.1 Have you identified all the categories of personal data that you will be processing and how?	Yes ☐ No X☐
If yes, please list them. If no, please indicate why not.	The audit data set includes details of clinical advice and the patient experience of the data subject The objective is to ensure data quality of the image and correct application of the agreed Clinical Protocol. The CT images will be of patients held in existing Picture Archiving Communication Systems (PACS) instances of each participating Trust which are already covered in Data Sharing Agreements.
1.2.2 Have you identified the purposes for which you will be processing personal data and how?	Yes X☐ No ☐
If yes, please list them. If no, please indicate why not.	Health Administration and Services (see notification Z5544053)
1.2.3 Have you identified which of the grounds in Schedule 2 you will be relying on as providing a legitimate basis for processing personal data?	YesX ☐ No ☐
If yes, please list them. If no, please indicate why not.	1,4
1.2.4 Are you relying on different grounds for different categories of personal data?	Yes ☐ No X☐
If yes, how will this assessment be made?	

1.3 Schedule 3 - Grounds for Legitimate Processing of Sensitive Personal Data

If this project does not involve the processing of sensitive personal data, please go to section 1.4

1.3.1 Have you identified the categories of sensitive personal data that you will be processing?	Yes X☐ No ☐
If yes, can you list them. If no, please indicate why not.	Medical treatment

1.3.2 Have you identified the purposes for which you will be processing sensitive personal data?	Yes X ☐ No ☐
If yes, can you list them. If no, please indicate why not.	As 1.2.2 above
1.3.3 Have you identified which of the grounds in Schedule 3 you will be relying on as providing a legitimate basis for processing sensitive personal data?	Yes X ☐ No ☐
If yes, can you list them. If no, please indicate why not.	8
1.3.4 Are you relying on different grounds for different categories of sensitive personal data?	Yes ☐ No X ☐
If so, how will this assessment be made?	

1.4 Obtaining consent

1.4.1 Are you relying on the individual to provide consent to the processing as grounds for satisfying Schedule 2?	Yes ☐ No X ☐
If yes, when and how will that consent obtained?	
1.4.2 For the processing of sensitive personal data, are you relying on explicit consent as specified in Schedule 3, s1 of the Data Protection Act?	Yes ☐ NoX ☐
If so, when and how will that consent obtained?	

1.5 Lawful Processing

a. If you are a public sector organisation:

1.5.1 Does your processing of personal data fall within your statutory powers?	Yes X ☐ No ☐
If yes, please state what they will be. If no, please indicate why not.	As defined in the North Cumbria Acute Hospitals National Health Servcie Trust (Establishment Order 2001 as amended and as in equivalent Statutory Instruments relating to other NHS Trusts and Foundation Trusts made under the applicable NHS Acts.
1.5.2 How is compliance with the Human Rights Act being assessed?	

b. All organisations:

1.5.3 Are you assessing whether any of the personal data being processed is held under a duty of confidentiality?	Yes X ☐ No ☐
If yes, how will that assessment made? If no, please indicate why not.	All PID is processed under duty of confidentiality
1.5.4 How is that confidentiality maintained? (e.g. instructions on disclosure or shredding)	Security and policy controls in respect of the application and (N3) networking environment in place with each participating Trust who will all be compliant with the NHS Information Governance Assurance Statement, also review of supplier's Information Governance processes as required. Media disposal guidelines in place but are unlikely to be relevant to the Telestroke service.
1.5.5 Are you assessing whether your processing is subject to any other legal or regulatory duties?	Yes ☐ No X ☐
If yes, how is that assessment being made? If no, please indicate why not.	Not applicable
1.5.6 How are you ensuring that those legal duties are being complied with?	

1.6 Fair Processing

1.6.1 Are individuals being made aware of the identity of your organisation as the data controller?	Yes X ☐ No ☐
If yes, state how they are being made aware. If no, please indicate why not.	A specific leaflet for Telestroke patients and their relatives is being prepared in addition to general leaflet "Information for Patients" and the Fair Processing Notice (FPN). Media/content may vary in each participating Trust
1.6.2 How are individuals being made aware of how their personal data is being used?	As above
1.6.3 How are individuals offered the opportunity to restrict processing for other purposes?	The leaflet and FPN refer to this
When is that opportunity offered?	
1.6.4 Do you receive information about individuals from third parties?	Yes X ☐ No ☐
If yes, please give examples. **If no, please go to section 1.7**	Northwest Ambulance Service NHS Trust pre-alert to A&E
1.6.5 How are individuals informed that the data controller is holding personal data about them?	See 1.6.2
When are individuals informed?	See 1.6.2

1.7 Exemptions from the First Data Protection Principle

The Act requires that in order for personal data to be processed fairly, a data controller must provide the data subject with the following information:-

1. the identity of the data controller

2. the identify of any nominated data protection representative, where one has been appointed

3. the purpose(s) for which the data are intended to be processed

4. any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

Data Protection Act, Schedule 1, Part II, para. 2 (3)

1.7.1 Do you provide individuals with all of the information in the box above?	YesX ☐ No ☐
If no, which exemption to these provisions is being relied upon?	

2 Principle 2: Purpose Limitation

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

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 35-6

2.1 Uses of Personal Data within the Organisation

2.1.1 Are procedures in place for maintaining a comprehensive and up-to-date record of use of personal data?	Yes X ☐ No ☐
2.1.2 How often is this record checked?	Continually
2.1.3 Does the record cover processing carried out on your behalf (e.g. by a subcontractor)?	YesX ☐ No ☐
2.1.4 What is the procedure for notifying (where necessary) the data subject of the purpose for processing their personal data? (Cross reference with section 1.6, Fair Processing)	See 1.6 new leaflet will explain the purpose of the service and the benefits , existing leaflet explains to all patients the data controller (Trust)'s purposes for processing their data

2.2 Use of Existing Personal Data for New Purposes

2.2.1 Does the project involve the use of existing personal data for new purposes?	Yes ☐ No X☐ **If no, go to section 2.3**
2.2.2 How is the use of existing personal data for new purposes being communicated to:-	
(a) the data subject;	
(b) the person responsible for Notification within the organisation	
(c) the Information Commissioner?	
2.2.3 What checks are being made to ensure that further processing is not incompatible with its original purpose?	

2.3 Disclosures of Data

2.3.1 Do you have a policy on disclosures of personal data within your organisation/to third parties?	YesX☐ No ☐
Is it documented?	Yes X☐ No ☐
2.3.2 How are staff made aware of this policy/instructed to make disclosures?	The policy is published on the Intranet (“Staffweb”) – periodic revisions are notified via e-mail and training is provided to key staff. Information Governance e-learning mandated for all staff provides general guidance on inappropriate disclosure.
2.3.3 How are individuals/data subjects made aware of disclosures of their personal data?	The FPN and notification indicate general basis of disclosure. The leaflet for patients in respect of the new service will refer to its benefits and the access to images given via secure remote access to the on call Stroke Specialist who may working for another NHS Trust
2.3.4 Do you assess the compatibility of a 3rd party's use of the personal data to be disclosed?	Yes ☐ No X☐ **If no, go to section 3.1**

If yes, how do you make the assessment?	

3 Principle 3: Adequate, Relevant and Not Excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 36-37

3.1 Adequacy and relevance of Personal Data

3.1.1 How is the adequacy of personal data for each purpose determined? (Please give examples.)	The requirement is to access images for the purpose of clinical diagnosis and to record minimal patient information to support quality assurance and audit processes
3.1.2 How is an assessment made as to the relevance (i.e. no more than the minimum required) of personal data for the purpose for which it is collected?	The requirement has been assessed by the clinical leads
3.1.3 What procedures are in place for periodically checking that data collection procedures are adequate, relevant and not excessive in relation to the purpose for which data are being processed?	There will be regular meetings of the lead provider/contracted supplier which will ensure that the data collection meets the purpose.
How often will these procedures reviewed?	
3.1.4 Are there procedures for assessing the amount and type of personal data collected for a particular purpose?	Yes ☐ No X ☐
If yes, please describe. If no, please indicate why not.	As indicated above the processing is primarily of clinical images
3.1.5 Are items of personal data held in every case which are only relevant to a subset of those cases?	Yes ☐ NoX ☐

4 Principle 4: Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date. **For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 37-8**

4.1 Accuracy of Personal Data

4.1.1 Are personal data evaluated to establish the degree of damage to both the data subject / data controller that could be caused through inaccuracy?	Yes ☐ No X ☐
4.1.2 How, and how often, are personal data be checked for accuracy?	The audit data mainly relates to calibration and other image quality assurance issues which are to enable a check on accuracy
Please give examples:	
4.1.3 In what circumstances is the accuracy of the personal data being checked with the Data Subject?	As per current procedures in A&E to ensure that patients are correctly identified and thereby registration on the related systems are either updated or created. All patients will present in A&E and then require a CT scan
Please give examples:	A&E, Patient Administration and Radiology Information Systems all include processes to check accuracy relating to Stroke patients
4.1.4 Are the sources of personal data (i.e. Data Subject, Data User, or third party) identified in the record?	Yes ☐ No X ☐
If so, how? Please give examples:	
4.1.5 Is there any facility to record notifications received from the data subject if they believe their data to be inaccurate?	YesX ☐ No ☐
If no, please indicate why not.	

4.2 Keeping Personal Data Up to Date

4.2.1 Are there procedures to determine when and how often personal data requires updating?	Not applicable – image and supporting data captured for immediate use in emergency treatment.
4.2.2 Are personal data evaluated to establish the degree of damage to:	
(a) the data subject, or (b) the data controller, that could be caused through being out of date?	Yes ☐ NoX ☐
Please specify whether to data subject or data controller:	
4.2.3 Are there procedures to monitor the factual relevance, accuracy and timeliness of free text options or other comments about individuals?	Yes ☐ No X ☐

5 Principle 5: No Longer than Necessary

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. **For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance p 39**

5.1 Retention Policy

5.1.1 What are the criteria for determining retention periods of personal data?	The Trust policy follows the NHS Code of Practice for Records Management Part 2 Annex D1
How often are these criteria reviewed?	Approximately every 3 years
5.1.2 Does the project(s) include the facility to set retention periods?	Yes ☐ No X ☐

5.1.3 Is the project subject to any statutory/sectoral requirements on retention?	Yes X ☐ No ☐
If yes, please state relevant requirements:	Image retention 8 years unless otherwise indicated

5.2 Review and Deletion of Personal Data

5.2.1 Is there a review policy?	Yes ☐ No X ☐
Is it documented?	Yes ☐ No ☐
5.2.2 When data is no longer necessary for the purposes for which it was collected:	
(a) How is a review made to determine whether the data should be deleted?	There is currently no functionality within the deployed Picture Archiving and Communication System (PACS environment) which supports the deletion of record life expired images
(b) How often is the review conducted?	See 5.2.2 (a) above
(c) Who is responsible for determining the review?	See 5.2.2. (a) above. Deletion of images would be the responsibility of the Information Asset Administrator for the relevant system.
(d) If the data is held on a computer, does the application include a facility to flag records for review / deletion?	Yes ☐ No X ☐
5.2.3 Are there be any exceptional circumstances for retaining certain data for longer than the normal period?	Yes ☐ No X ☐
If yes, please give justification:	

5.2.4 Is there any guidance on deletion/destruction of personal data?	Yes X ☐ No ☐
If no, please indicate why not.	

6 Principle 6: Data subject access

Personal data shall be processed in accordance with the rights of data subjects under this Act. **For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 39-40**

6.1 Subject Access

6.1.1 Are procedures in place to provide access to records under this Principle?	YesX ☐ No ☐
If yes, please specify proposed procedures. If no, please indicate why not.	As per existing Data Protection Policies and Procedures for each participating Trust. NCUHT responsible as Data Controller for overarching Audit record
6.1.2 How do you locate all personal data relevant to a request (including any appropriate 'accessible' records)?	All image records indexed on Trust Radiology Information System
6.1.3 Do you provide an explanation of any codes or other information likely to be unintelligible to a data subject?	YesX ☐ No ☐
If yes, how? If no, please indicate why not.	Supplied on request – unlikely to apply in respect of CT images
6.1.4 Are procedures in place to manage personal data relating to third parties?	Yes ☐ No X ☐
If yes, please specify proposed procedures. If no, please indicate why not.	Not relevant – data subjects will either be patients or members of staff of the participating Trusts whose identity will be known to patients as part of the clinical assessment process
6.1.5 How is data relating to third parties managed?	Not applicable

6.2 Withholding of personal data in response to a subject access request

6.2.1 Are there any circumstances where you would withhold personal data from a subject access request?	Yes X ☐ No ☐
If no, go to section 6.3. If yes, on what grounds?	Technically possible in terms of S.30 & SI 2000 no 413 The Data Protection (Subject Access Modification (Health) Order 2000) but no likely circumstance for its application is foreseen.
6.2.2 How are the grounds for doing so identified?	All Subject Access Requests are routinely reviewed for possible application of S.30

6.3 Processing that may cause Damage or Distress

6.3.1 Do you assess how to avoid causing unwarranted or substantial damage or unwarranted and substantial distress to an individual?	Yes ☐ NoX ☐
If yes, please specify proposed procedures. If no, please indicate why not.	Not applicable
6.3.2 Do you take into account the possibility that such damage or distress to the individual could leave your organisation vulnerable to a compensation claim in a civil court?	Yes ☐ NoX ☐

6.4 Right to Object

6.4.1 Is there a procedure for complying with an individual's request to prevent processing for the purposes of direct marketing?	Yes ☐ No X ☐

6.5 Automated Decision-Taking

6.5.1 Are any decisions affecting individuals made solely on processing by automatic means?	Yes ☐ NoX ☐

If yes, what will be the procedure(s) for notifying an individual that an automated decision making process has been used?	

6.6 Rectification, Blocking, Erasure and Destruction

6.6.1 What is the procedure for responding data subject's notice (in respect of accessible records) or a court order requiring:	
(a) rectification;	Standard Trust Policy/Procedure if S.10 notice received
(b) blocking;	As above
(c) erasure or;	If required by order of Tribunal
(d) destruction of personal data?	If required by order of tribunal

7 Principle 7: Data Security

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.

For the Information Commissioner's guidance in relation to this DPP, see Legal Guidance pp 40-3

7.1 Security Policy

7.1.1 Is there a Data Security Policy?	Yes X ☐ No ☐
If no, please indicate why not and then go to 7.1, question 5.	

7.1.2 If yes, who/which department(s) are responsible for drafting and enforcing the Data Security Policy within the organisation?	IM&T Directorate/Informatics Security Officer
7.1.3 Does the Data Security Policy specifically address data protection issues?	Yes X ☐ No ☐
7.1.4 What are the procedures for monitoring compliance with the Data Security Policy within the organisation?	Application of Incident Reporting Policy, Review of Serious Untoward Incidents, Reports to Information Governance Group
7.1.5 Does the level of security that has been set take into account the state of technological development in security products and the cost of deploying or updating these?	Yes
7.1.6 Is the level of security appropriate for the type of personal data processed?	Yes
7.1.7 How does the level of security compare to industry standards, if any?	Processing undertaken by N3 Information Governance Assurance Statement compliant organisations

7.2 Unauthorised or unlawful processing of data

7.2.1 Describe security measures that are in place to prevent any unauthorised or unlawful processing of:	
(a) Data held in an automated format (e.g. password controlled access to PCs)	Access to Telecart and remote PCs subject to procedures compliant with NHS Information Governance Requirements 305 (Access Controls and Controls Functionality) and 314 (Mobile Computing and Teleworking)
(b) Data held in a manual record (e.g. locked filing cabinets)	Not applicable

7.2.2 Is there a higher degree of security to protect sensitive personal data from unauthorised or unlawful processing?	Yes ☐ NoX ☐
If yes, please describe the planned procedures. If no, please indicate why not.	
7.2.3 Describe the procedures in place to detect breaches of security (remote, physical or logical)?	Standard firewall configuration within each COIN for participating Trust and N3 in respect of the external facing environment

7.4 Destruction of Personal Data

Cross-reference with section 5.2

7.4.1 Describe the procedures in place to ensure the destruction of personal data no longer necessary?	See comments in 5.2. Data and images will be retained for 8 years
7.4.2 Are there different procedures for destroying sensitive personal data?	Yes ☐ No X ☐

7.5 Contingency Planning - Accidental loss, destruction, damage to personal data

7.5.1 Is there a contingency plan to manage the effect(s) of an unforeseen event?	Yes X☐ No ☐
7.5.2 Describe risk management procedures to recover data (both automated and manual) which may be damaged/lost through:	
• human error	Database can be restored from back ups,
• computer virus	Standard Virus Protection measures will be in place.
• network failure	Single Points of failure eliminated where possible. In the event of total loss of network access clinicians will revert to original working practices.
• theft	Not applicable

• fire	Not applicable – service is spread across multiple networks and data centres.
• flood	Not applicable – service is spread across multiple networks and data centres.
• other disaster.	

8 Principle 8: Overseas Transfer

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

For the Information Commissioner's guidance in relation to this Legal Guidance DPP, see pp 43-5

8.1 Adequate Levels of Protection

8.1.1 Are you transferring personal data to a country or territory outside of the EEA?	Yes ☐ No X ☐ **If no, please go to Part III.**
If yes, where?	
8.1.2 What are the types of data are transferred? (e.g. contact details, employee records)	
8.1.3 Are sensitive personal data transferred abroad?	Yes ☐ No ☐
If yes, please provide details:	
8.1.4 What are the main risks involved in the transfer of personal data to countries outside the EEA?	

8.1.5 Are measures in place to ensure an adequate level of security when the data are transferred to another country or territory?	
8.1.6 Have you checked whether any non-EEA states to which data is to be transferred have been deemed as having adequate protection?	

8.2 Exempt Transfers

8.2.1 Is your organisation carrying out any transfers of data where it has been decided that the Eighth Principle does not apply?	Yes ☐ No ☐
If yes, what are they?	
8.2.2 To which country / territory are these transfers made?	
8.2.3 What are the criteria set by your organisation, which must be satisfied before a decision is made about whether the transfer is exempt from the Eighth Principle? E.g. consent, (See DPA 1998, Schedule 4, for a full list)	

8.3 Choosing a Data Processor

8.3.1 What reasonable steps did you take to ensure that the Data Processor complies with data protection requirements?	
8.3.2 How did you assess their data security measures?	
8.3.3 How do you ensure that the Data Processor complies with these measures?	

8.3.4 Is there an on-going procedure for monitoring their data security measures?	Yes ☐ No ☐
If yes, please describe. If no, please indicate why not.	

III DPP COMPLIANCE – CONCLUSIONS

Please provide a summary of the conclusions that have been reached in relation to this project's overall compliance with the DPPs. This could include indicating whether some changes or refinements to the project might be warranted.

Further work is required to ensure that the PACS which stores the CT image used by the Telestroke Service fully complies with the 5th principle in terms of functionality which allows the selection and automated deletion of images which exceed NHS Records Management Code of Practice/Trust retention policy limits

_____ Service Manager Title_____ Date: _____

_____Data Protection Officer Title_____ Date: _____