ACHE- Carpal Tunnel Service At Victoria Park Health Centre

Data Protection Impact Assessment (DPIA)

Data Protection Issue	What Policies Apply	Assessment of Risk	Mitigation Measures	Conclusion
Purpose Specification **1. Why are you collecting this data** The data is being collected for the delivery of an orthopaedic hand service that will include diagnostic nerve conduction study, an appointment and possible carpal tunnel decompression procedure **2. Is the data to be collected to be used for a specified purpose only** Yes for safe delivery of the Hand Surgery Service	Clinical Governance GDPR Caldicott Data Protection Policy	Low Risk and low impact Minimal and acceptable as we cannot provide the service without this information	Training Dissemination of policies Signing of confidentiality agreements Data sharing agreements	Continue with regular review
Data limitation **1. Is all the personal data collected necessary for the stated activity?** Yes we must be able to identify patients and share outcomes with the referring practice **2. When patients use the service, are they told how the personal information supplied will be used?** Yes it is a GDPR contractual obligation to do so	Caldicott GDPR Consent for Share Information Data Protection	Low Risk and low impact Minimal and acceptable as we cannot provide the service without this information	Signed consent form for data sharing that explains how the information will be used	Continue with regular review and keep copies of signed consents on patients records

Right to information 1. **Are individuals explicitly informed about why their personal data is being collected and how it may be used?** Yes it is a GDPR contractual obligation to do so	GDPR	Low Risk and low impact	N/A	Signed consent form for data sharing that explains how the information will be used
Legal basis for data processing/transfer **Consent** 1. **Are individuals able to appreciate the most likely consequences (including negative)?** Yes they are provided information regarding the diagnosis and procedure before their appointment, and consent is gained again during each patient contact with a clinician. 2. **Does the processing involve complex technologies?** No, we are using accredited NHS Systems that are known to general practice with fail safes in place for data recovery and loss of service 3. **Does the person have a genuine free choice as to whether to consent?** Yes, consent is explicit and the consent form must be signed by the patient and operating surgeon 4. **How do individuals provide consent for their information to be collected?** They will be provided with a consent form, of which they retain a copy of.	Patient information leaflet regarding procedure pre appointment. Consultation with clinician to go through risks and outcomes Information Governance Policy Caldicott Policy Computer Misuse Act 1990 Written consent required to proceed Written consent required to proceed	Low Risk and low impact Small Risk of procedure failure Low Risk but high impact Small risk but we have Data recovery and business continuity plans in place to ensure safety of data Low Risk and medium impact No risk as process will not proceed without consent, may impact on patient expectation Low Risk and medium impact No risk as process will not proceed without consent	Signed consent for the procedure that also outlines the risk Review of business continuity plans on an annual basis or when the process changes Scan evidence of consent onto patients medical record Scan evidence of consent onto patients medical record	Signed consents must be retained and scanned on to the patients record

5. Is consent limited to a specified purpose? Yes for the communication of information regarding outcomes to the referring GP and for reporting to the commissioner for payment and activity details **6. Will the individual explicitly agreed to how their information can be used, or that it can be shared with other agencies?** Yes, they will also be asked to sign a consent form giving agreement for consent	Consent form describes data sharing and procedure Consent form describes data sharing and procedure	Low Risk and medium impact process will not proceed without consent Low Risk and medium impact process will not proceed without consent	Scan and read code evidence of consent onto patients medical record Scan and read code evidence of consent onto patients medical record	
<u>Right to access / Rectification / Deletion</u> **1. Are individuals provided with the possibility to access and correct their personal information?** If this is the case, it will be reported to the referring GP who is the main controller of the patient data. **2. Can they request the deletion of some or all of their personal information?** No, special category data is exempt from this Clause. Extract GDPR- Special category Data '(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;'	GDPR Policy GDPR	Medium Risk Low Impact Potential risk, but we will report the SUI to the referring practice as a GDPR concern N/A The right to erasure does not apply Extract from GDPR; 'if the processing is necessary for the purposes of preventative or occupational medicine (eg where the processing is necessary for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services). This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health	N/A	GDPR regulations must be observed

		professional).’		
Information quality and accuracy **1. What processes are in place for ensuring information quality, i.e., that the information is relevant, reliable, accurate and actionable?** The process will be underpinned by other Information Governance Policies	Caldicott Data Protection GDPR	Low Risk and medium impact There is a risk but this will be manged by training and regular audit of information collected	Audit and staff training	Annual training updates and regular audit required
Appropriate security measures **1. What personal information is to be collected? Could disclosure of this information put the person in danger?** Name, DOB, Address and GP, disclosure of this information could cause a risk to the patient. **2. Is there a risk of information being stolen / lost / altered / rendered unavailable / system hacked / organisation subject to surveillance?** There is always an element of risk but it is minimal and the service has robust monitoring processes in place to ensure data safety **3. What preventative measures are in place?**	Data Protection GDPR Data Protection Computer Misuse Act 1990 Practice computer hardware Policy Data Protection Computer Misuse Act 1990	Low Risk but high impact The data shared outside the organisation will be shared via NHS accredited systems that have robust firewalls and malware identifiers	The data shared outside the organisation will be shred via NHS accredited systems that have robust firewalls and malware identifiers Staff training on computer safety	Adhere to the NHS and Practice policies for use of computers

Audits, training, confidentiality agreements, data sharing agreements	Practice computer hardware Policy Staff training and IT use audits	Staff training and IT use audits	Staff training on computer safety	Monitor computer use and access to records
4. Does the processing involve external organisations or third parties? Yes	All organisations that are commissioned by the NHS	Low Risk but high impact Breach of data is low, but would be significant to the patient if there was a data breach		
5. Does this increase the risk of surveillance / disclosure by the processor (whether lawfully or not) / hacking / data theft / availability? No, all systems are NHS accredited and secure				
6. Is information limited to others on a "need to know"? How is this implemented in practice? Records and data will be 'locked down' to only be visible by staff who are directly involved in the delivery of the service	Caldicott Data Protection Managing patient records	Low Risk but high impact	Staff training on Caldicott Principles	Monitor record access and ensure staff are aware that any unlawful access to patient data is a disciplinary offence
7. Is training given to all staff on good data protection and information security practices? Yes	Blue Stream or other NHS accredited online learning system	Staff training and IT use audits	Blue Stream or other NHS accredited online learning system	Ensure all relevant staff update training annually or as and when processes change
8. What action will be taken if there is a data breach? This will be as GDPR regulates				
9. Are individuals informed if their personal data is lost, stolen or other compromised?	Caldicott Data Protection GDPR			

Yes this is a GDPR requirement **10. Will any other organisations be informed?** Yes, this is a GDPR requirement, LLR PCL, ACHE and ICO		Inform ICO within 72 hours of breach	Staff training on GDPR	Review data processes with DPO
<u>Data sharing, disclosure/publication/ and/or transfer</u> **1. Will the personal information be shared with or disclosed to other organisations? Why?** The personal information will only be shared with the referring practice as this is part of the patients health journey, **2. Have they provided written assurances that they will safeguard the information and not share it further?** Yes all GP practices are regulated and governed by GDPR **3. Does the organisation have an adequate data protection policy?** Yes	Caldicott Data Protection GDPR Management of patient records Data Sharing Agreement	Low Risk and low impact All NHS accredited systems which are safe to transfer patient identifiable data Low Risk but high impact Information should be shared safely providing all processes are followed, so the risk of breach is low. Should there be an unintentional breach, this could have a high impact on the patient	DPO assessment of data sharing processes	DPO process audit on a quarterly basis
<u>Data retention</u> **1. Is personal information being entered**	SystemOne	Low Risk and low impact		

into databases? Yes it is input into the practices clinical system **2. Is it necessary to keep all of the data that is being processed?** Yes **3. Are there procedures for reviewing how long data should be retained?** All medical data needs to be retained for the duration of the patients life, but will not be accessible after discharge from the service	GDPR retention rules apply		Data quality checks to ensure standardised methods of data input are being used to ensure accuracy and appropriateness of data	DPO process audit on a quarterly basis
<u>Accountability/Oversight mechanism:</u> **1. Are data protection standards and procedures effectively implemented?** Yes **2. Are oversight mechanisms in place to overview existing practices and to provide guidance to the ACHE Site?** Yes we have a DPO	GDPR regulations	Medium risk high impact Regular data monitoring and quality checks must be performed		DPO process audit on a quarterly basis