THE ELMS MEDICAL PRACTICE
16 Derby Street, Ormskirk, L39 2BY Tel: 01695 588710

Dr A. Krishnamurthy. MBBS MRCGP & Dr G. Duddukuri. MBBS MRCGP
Sister Cathy Evans ANP & Sister Paula Tynan

The Data Protection Impact Assessment

This document is to be used to conduct a DPIA at The Elms Medical Practice.

Step 1 – Determining the need – overall assessment of practice

Does the process involve any of the following:	YES	NO
The collection, use or sharing of existing data subjects' health information?	X	
The collection, use or sharing of additional data subjects' health information?	X	
The use of existing health information for a new purpose?	X	
The sharing of data subjects' health information between organisations?	X	
The linking or matching of data subjects' health information which is already held?	X	
The creation of a database or register which contains data subjects' health information?	X	
The sharing of data subjects' health information for the purpose of research or studies (regardless of whether the information is anonymised)?		X
The introduction of new practice policies and protocols relating to the use of data subjects' personal information?	X	
The introduction of new technology in relation to the use of data subjects' personal information, i.e. new IT systems, phone lines, online access, etc?	X	
Any other process involving data subjects' health information which presents a risk to their "rights and freedoms"?		X

If the answer is yes to one or more of the above questions, a DPIA is required. Proceed to Step 2.

Step 2 – Assessing the risks

Information collection – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject	
What information is being collected and how?	Healthcare and Data subject information. Electronic systems:- Emis clinical system Docman10 document system iPlato – communication system OOHs clinical system
Where is the information being collected from and why?	Electronic pathways / IT Systems. To support healthcare provision to patients.
How often is the information being collected?	At point of consultation(s)
Information use – Is the data obtained for specified, explicit and legitimate purposes?	
What is the purpose for using the information?	Data processes including:- Patient healthcare Referrals Reviews of medication Communication
When and how will the information be processed?	Consultations Emis clinical system
Is the use of the information linked to the reason(s) for the information being collected?	YES
Information attributes – Personal data shall be accurate and, where necessary, kept up to date	
What is the process for ensuring the accuracy of data?	To provide correct healthcare. Confirm data subjects' details. Using the correct data subject. Practice policies and protocols for clinical coding, summarising and work flowing (scanned documents)
What are the consequences if data is inaccurate?	Communications not being followed up – delay in treatment. Patient being give the wrong health advise – causing an adverse impact on patient health.
How will processes ensure that only extant data will be disclosed?	Templates in place within Emis Confidentiality protocol Consent form patient or their representative(s).
Information security – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
What security processes are in place to protect the data?	Smart cards and RBAC. Computer locks. Confidentiality policy, GDPR policy, consent policy, staff training.
What controls are in place to safeguard only authorised access to the	All record access is fully auditable within the clinical system . Regular

data?	coding spot checks. Practice policy on security (computer locking / non sharing of passwords etc). Regular staff training.
How is data transferred; is the process safe and effective?	End to end encryption – GP2GP. Owls. Docman, AccuRx. Approved by WLCCG and MLCSU through DPIA and certification.
Data subject access – Personal data shall be accurate and, where necessary, kept up to date	
What processes are in place for data subject access?	Data subjects can complete a form to request SAR – even if done through a solicitor. Identity is necessary. Online access only provided with photo ID.
How can data subjects verify the lawfulness of the processing of data held about them?	Data subjects can view their medical records. Audit trails available on request.
How do data subjects request that inaccuracies are rectified?	Request to speak with the data controller.
Information disclosure – Personal data shall be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	
Will information be shared outside the practice; are data subjects made aware of this?	Yes. Consent requested from patient eg before a referral. Privacy policy to be adhered to.
Why will this information be shared; is this explained to data subjects?	Yes – consent requested before sharing eg referral. To facilitate ongoing treatment and examination of data subject.
Are there robust procedures in place for third-party requests which prevent unauthorised access?	SAR request form solicitor always followed up with practices' own form explaining what will be available to the solicitor or/and courts. Parental responsibility requested if patient under 13 and/or not Gillick assured. Consent/authority needed from data subject.
Retention of data – Personal data shall be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed	
What are the retention periods associated with the data?	See Retention Policy / Summarising policy for guidance on retention schedules.
What is the disposal process and how is this done in a secure manner?	After retention period the records can be reviewed and if no longer needed destroyed. Certificate of destruction required Manual Medical records of data subjects who have died are returned to PCSE.
Where is data stored? If data is moved off-site, what is the process; how can data security be assured?	Data subject medical records are stored electronically on Emis. Lloyd George Medical records are stored via NoteSpace / Niche Health. Data security is provided by this company under the depositor agreement.

Step 3 – Risk mitigation

Information collection – The risk
Personal data is collected without reason or purpose – increased risk of disclosure.
Information collection – The mitigation
The reasons for data collection must be clearly stated and all personnel must understand why the data has been collected.
Information use – The risk
Personal data is used for reasons not explained to, or expected by, the data subjects.
Information use – The mitigation
Clearly explain and display to data subjects how their information will be used. Data-sharing requires a positive action, i.e. opting in, not opting out!
Information attributes – The risk
Data is inaccurate or not related to the data subject.
Information attributes – The mitigation
Make sure robust procedures are in place to ensure the data held about data subjects is accurate, up to date and reflects the requirements of the data subject for which it was intended.
Information security – The risk
Unauthorised access to data due to a lack of effective controls or lapses of security/procedure.
Information security – The mitigation
Ensure that staff are aware of the requirement to adhere to the practice's security protocols and policies; conduct training to enhance current controls.

Data subject access – The risk
Data subjects are unable to access information held about them or to determine if it is being processed lawfully.
Data subject access – The mitigation
Ensure that data subjects are aware of access to online services and know the procedure to request that information held be amended to correct any inaccuracies.
Information disclosure – The risk
Redacting information before disclosure might not prevent data subjects being identified – i.e. reference to the data subject may be made within the details of a consultation or referral letter.
Information disclosure – The mitigation
Make sure the policy for disclosure is robust enough to ensure that identifying information is removed.
Retention of data – The risk
Data is retained longer than required or the correct disposal process is not adhered to.
Retention of data – The mitigation
Ensure that practice policies and protocols clearly stipulate data retention periods and disposal processes. Review and update protocols and policies and, if necessary, provide training for staff to ensure compliance.