Data Privacy Impact Assessment - E-clinic patient management system

What is the processing Activity (Describe in detail the processing activity to be carried out on behalf of HEM Clinical Ultrasound Service LTD.	LEVEL OF RISK
e-clinic Pro patient management has been contracted to provide a patient management system upon which we store all patient data. We utilize most aspects of the software for our day to day patient management needs. Patient data stored on the system is divided into 'personal information' and 'Sensitive personal information' and is as follows (Question one answered – What type of information will need processing): **Personal Information:** Full Name, Date of birth, Gender, NHS Number, Address, Telephone number/s, GP Practice and address. Consent form verifying personal details. **Sensitive personal Information:** Clinical Indication on the referral form, Including relevant medical history, Patient appointment letters detailing scan type and preparation, Patient reports detailing outcome of examination and recommendations for onward referral, Clinical images – containing imaged organs and findings of pathology. Patient notes detailing pertinent patient details such as compliments and complaints or personal disabilities, Patient billing records, appointment times and requests. **The data held on e-clinic is processed in the following manner** (Question Two answered – How is the data processed): **BY HEM:** 1. 'Personal Information' is utilised to create the patient profile manually entering the demographics and saving to create the patient profile. 2. The patients referral form is uploaded and saved as a PDF following triage 3. Triage and preparation noted on the 'Notes' 4. Patient appointment booking noted on 'Notes'	Processing : 'Is likely to result in a high risk to the rights and freedoms of a natural person' (As stated by the DPIA GDPR Article 29 working party guidance)

5. Patient appointment time set and letter generated (If letter booking) Letter saved and printed. 6. Patient consent form is saved prior to appointment 7. Patient report written and saved on system – PDF'd and sent to the referrer by Operations manager/Senior team 8. Patient Images uploaded to system in a zipped folder for storage. 9. Additional notes kept up to date of any information requests, complaints compliments or queries by referrers or data subjects. How much information is stored? There are in excess of 27,500 patients stored on e-clinic.	
The data held on e-clinic is processed in the following manner: **BY E-CLINIC:** 1. For storage by a subcontractor in a ISO27001 Compliant Data centre. Information is encrypted and sent securely for storage. How much information is stored? (Question number three answered – how much data is stored) There are in excess of 27,500 patients stored on e-clinic. 2. E-clinic staff manage support and guidance to HEM Clerical team for resolution of any issues – such as incorrect data stored, Patient profile merging, program glitches and continual improvement. This support requires access to patient profiles.	Processing : 'Is likely to result in a high risk to the rights and freedoms of a natural person' (As stated by the DPIA GDPR Article 29 working party guidance)

What are the hazards?	Who might be harmed and how?	What are you already doing?	Do you need to do anything else to control this risk?	Action by who?	Action by when?	Done
Does the Data Processer have the following security controls: Secure storage solutions to DPA Standards	In the event of a data breach, loss of Data, or malicious attack the data level is considered 'Critical' which means: - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic. This data processing agreement includes a clause regarding secure storage of Data. And the e-clinic data center is ISO 27001 compliant.	The risks are low as the storage of the data is: Secure Backed up Easily accessible to HEM Staff	HEM Management team	Actioned at start of service with e-clinic	Risk managed
Staff Security checked to DBS level	In the event of mismanagement of patient data from staff not appropriately vetted: - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic this ensures compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data Assurance from e-clinic as to: - Appropriate background checks on staff with access to patient information	No- As part of their revised T&C's May 2018	HEM Management team	May 2018	Risk Managed

Staff have appropriate training and awareness of Data protection and confidentiality	In the event of mismanagement of patient data from staff not appropriately trained: - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data by staff of e-clinic. HEM Staff have training in Confidentiality and data protection. Regular spot checks are carried out	Staff Data protection training confirmed as undertaken quarterly in line with updated policies.	HEM Management team	Confirmed 29.03.2019	Risk Managed
Do they have a registered Caldicott guardian or Data Protection Officer– e-clinic	In the event of mismanagement of patient data from unstructured approach to information governance from nominated persons: - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data. Data Protection Officer and Caldicott is Mark Lainchbury	No Confirmed 29.03.2019	HEM Management team	No Confirmed 29.03.2019	Risk Managed
Are their policies and procedures compliant with the DPA and GDPR	Do they employ best practice, GDPR and DPA legislative guidance to their day to day data protection practices and overarching practices? - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data.	Confirmed within the T&C's and Quarterly updates and reviews completed	HEM Management team	No Confirmed 29.03.2019	Risk Managed

Do they process any information outside of the EU	Do they have the capability to process information outside the EU without prior approval from the Data controller? - Risk to individual service users - Risk to provision of service - Risk to company reputation	The company has service agreement (in the form of signed T&C's) validated by a solicitor with e-clinic which includes compliance with the principles of the data protection act and GDPR and restricts the processing of information outside of the EU	The Service agreement restricts the processing of information outside of the EU.	HEM Management Team	Actioned as part of our service agreement.	Risk Managed

From completion of the Data protection Impact assessment of e-clinic pro patient management there are clear areas for action and improvement prior. These areas for improvement will be implemented and agreed following the annual revision of the data processing agreement. Further action may be needed should controls not be sufficient.

E-clinic & HEM T&C's: The T&C's/Service agreement sets out the relationship between the 'Data Controller' (HEM) and the 'Data Processor' (e-clinic). The data processor must abide by the agreement with respect to the 'purpose' of the data processing and ensure they operate according to the law (GDPR and DPA) and stipulations made within any additional clause