

Data Privacy Impact Assessment - Medica Reporting Group LTD

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
<p>Medica Reporting Group Limited carry out monthly clinical audits of 5% of all ultrasound examinations undertaken out within our service.</p> <p>They have access to our patient management system – to enable them to view reports and referral forms for clinical validity. Access includes the following:</p> <p>Personal Information: Full Name, Date of birth, Gender, NHS Number, Address, Telephone number/s, GP Practice and address. Consent form verifying personal details.</p> <p>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.</p> <p>We also send images by secure dicom transfer to enable their clinicians to carry out the audits with the images stored on the Medica PAC’s system for a limited time.</p> <p>The data held by Medica is processed in the following manner</p> <ul style="list-style-type: none"> • Patient list is compiled by member of the HEM Team • Patients Images sent from the scanner to Medica PAC’s by secure transfer • Patient list anonymised and sent via e-mail to Medica team. • Medica team create job lists for Radiologists according to specialism 	<p>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)</p>

<ul style="list-style-type: none"> • These lists are sent to radiologists who have access to e-clinic and to Medica Pac’s system. • Radiologists record anonymised findings onto CAS system. • CAS Audit reports e-mailed to HEM Once audit completed. • Patients images deleted from Medica PAC’s after report finalised. <p>How much information is stored? Estimated to date Medica have received over 2000 patient details in order to carry out their audits.</p>	
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

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 a data processing agreement with Medica Reporting Group Limited – Validated by a Solicitor. This data processing agreement includes a clause regarding secure storage of Data.	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 Medica.	Risk managed

<p>Staff Security checked to DBS level</p>	<p>In the event of mismanagement of patient data from staff not appropriately vetted:</p> <ul style="list-style-type: none"> - Risk to individual service users - Risk to provision of service - Risk to company reputation 	<p>The Company has a data processing agreement with Medica Reporting Group Limited – Validated by a Solicitor which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data.</p>	<p>HEM Ultrasound has had physical assurances from Medica Reporting Group that staff with access to patient records have been properly vetted. Through a site visit.</p>	<p>HEM Management team</p>	<p>N/A</p>	<p>Risk Managed</p>
<p>Staff have appropriate training and awareness of Data protection and confidentiality</p>	<p>In the event of mismanagement of patient data from staff not appropriately trained:</p> <ul style="list-style-type: none"> - Risk to individual service users - Risk to provision of service - Risk to company reputation 	<p>The Company has a data processing agreement with Medica Reporting Group Limited– Validated by a Solicitor which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data by staff of Medica.</p>	<p>- Details of staff training in data protection and information handling obtained during site visit and confirmed as being updated annually</p>	<p>HEM Management team</p>	<p>N/A</p>	<p>Risk Managed</p>
<p>Do they have a registered Caldicott guardian or Data Protection Officer</p>	<p>In the event of mismanagement of patient data from unstructured approach to information governance from nominated persons:</p> <ul style="list-style-type: none"> - Risk to individual service users - Risk to provision of service - Risk to company reputation 	<p>The Company has a data processing agreement with Medica Reporting Group Limited – Validated by a Solicitor, which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data.</p>	<p>- Details of their Caldicott guardian and Data Protection Officer as a point of contact for IG issues:</p> <p>Caldicott: Simon Peele Data Protection Officer: Ian Edwards</p>	<p>HEM Management team</p>	<p>N/A</p>	<p>Risk Managed</p>
<p>Are their policies and procedures compliant with</p>	<p>Do they employ best practice, GDPR and DPA legislative guidance to their day to day</p>	<p>The Company has a data processing agreement with Medica Reporting Group Limited – Validated by a</p>	<p>Policies and procedures updated annually in line</p>	<p>HEM Management team</p>	<p>N/A</p>	<p>Risks Managed</p>

the DPA and GDPR	data protection practices and overarching practices - Risk to individual service users - Risk to provision of service - Risk to company reputation	Solicitor, which includes compliance with the principles of the data protection act and avoiding misuse and inappropriate handling of data.	with the GDPR and Data Protection Act.			
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 a data processing agreement with Medica Reporting Group Limited– Validated by a Solicitor which includes compliance with the principles of the data protection act and GDPR and restricts the processing of information outside of the EU.	The data processing agreement restricts the processing of information outside of the EU.	HEM Management team	Included with revised third party data protection agreement	Risk Managed

From completion of the Data privacy Impact assessment of Medica Group LTD show there are clear areas for action and improvement. 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.

The Data Processing agreement:

The Data processing agreement sets out the relationship between the ‘Data Controller’ (HEM) and the ‘Data Processor’ (Medica Group LTD). 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.

