Data Privacy Impact Assessment – CCG Billing Records

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
Data Includes: Case ID,NHS Number, Referral Received Date, Referral Type, Referring Practice, Referring Practice Code, Select, Category, Select Type, Appointment Date, Discharge Reason, Total Amount & Summary of total scans and procedures. **How is it processed?** Files are built up over time and they are stored on the NAS and as paper files in the TAMBA Unit.	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?	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 data is stored securely in the Synology Network attached Storage – the NAS backs up daily to an encrypted cloud storage solution.	**No**	**N/A**	**N/A**	**Yes**
Secure storage solutions to DPA Standards	In the event of mismanagement of patient data from staff not appropriately vetted:	The data is stored securely in the Synology Network attached Storage – the NAS backs up daily to an encrypted cloud storage solution.	**No**	**N/A**	**N/A**	**Yes**

	- Risk to individual service users - Risk to provision of service - Risk to company reputation					
Staff Security checked to DBS level	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 data is stored securely in the Synology Network attached Storage – the NAS backs up daily to an encrypted cloud storage solution. Logins for the Invoicing only for the Operations Manager and the SIRO both Checked with advanced DBS.	**No**	**N/A**	**N/A**	**Yes**
Staff have appropriate training and awareness of Data protection and confidentiality	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	Staff are aware of their responsibilities and have had training in information governance and data protection. The responsibility of maintaining the invoicing and billing files lies with the operations manager and Service Director who have a higher level of training and understanding of their responsibilities.	**No**	**N/A**	**N/A**	**Yes**
Do they have a registered Caldicott guardian and Data Protection officer	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	YES – Caldicott guardian and Data Protection Officer	**No**	**N/A**	**N/A**	**Yes**

Are their policies and procedures compliant with the DPA and GDPR	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	Policies have been reviewed in line with the GDPR and the Data protection act	No	N/A	N/A	Yes
Do they process any information outside of the EU	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	No Data is processed outside the EU	**N/A**	**N/A**	**N/A**	**Yes**