Clarity Medical Tele-Medicine Solution Data Privacy and Protection Audit Performed in Mar 2020	*Cloud Implementation*	*On Prem Implementation*
Audit Task List		
What is the type of data collected?	Trends/Waveforms/Patient data	Trends/Waveforms/Patient data
What are the sources of the data collected?	Patient monitors / Proximity Device / Central Monitoring Station.	Patient monitors / Proximity Device / Central Monitoring Station.
In what location is data held?	Proximity device/CMS and or the Cloud	Proximity device/CMS and or the Cloud
For what purpose is the data used?	Display only except trends are stored for upto 96 hours on the proximity / CMS.	Display only except trends are stored for upto 96 hours on CMS.
Is retention of data necessary?	Long term of retention data is not needed unless specifically requested.	Per customer direction.
What security measures are in place to protect the data?	256 bit encryption while in transmission. 128bit encryption when accessed thru a browser. All data is stored on 128 bit certificate protected cloud storage.	Encryption on the left apply with the caveat that physical assets are liable to be risks of being stolen and hence customer must demonsrate appropriate security or assume all risk.
Can be data be accessed and furnished to the individual concerned should they make a system access request?	Yes.	Yes.
Should it be needed can the data be easily deleted or destroyed?	Yes.	Yes.
What are the risks to the data collected?	Data loss / alteration / theft.	Data loss / alteration / theft.
How can these risks be identified?	Constantly monitor data-store for errors and access.	Customer responsiblity.
How can identified risks be mitigated?	Data store is replicated across storage servers.	Data can be replicated to an external hard-disk. Responsiblity of the customer. Software carries the provision.
In case of data breach do you have processes in place to notify the Data Protection Authority for each respective customer?	Yes.	No. On prem data protection is purview of customer.
Are data protection guidelines, risks to data, risk mitigation procedures, risk nofification procedures well documented within your organization?	Yes.	Yes.
How frequently are your data protection guidelines and processes reviewed?	Once a year.	Once a year.
Do you have a publicly accessible privacy policy outlining all the processes related to the collection, processing and maintenance of personal data?	Yes. On our website.	Yes. On our website.
Does your Privacy Policy explain the lawful basis why your organization needs to collect and process personal information?	Yes.	Yes.
Have you appointed a representative within the EU who will be responsible for reporting data breaches to the DPA and the data subjects whose data has been breached?	Yes.	Yes.
Has your organization put mechanisms in place to allow individuals to request access to their personal information, to update or correct it as necessary, to request their data is erased or transferred to another data processor?	Handled thru stakeholders	Handled thru stakeholders
Does your organization always ask for specific consent before processing an individual´s information, give them the opportunity to object to personal profiling or automated decision making that could impact them, and give them the right to easily withdraw their consent?	Handled thru stakeholders	Handled thru stakeholders