



Your organization's Business Continuity Plan is in place and tested at least every two years.

ENSURE you have a documented plan to address all systems and processes to minimize patient impact in an emergency.



All systems and technology are actively assessed for risk associated with data storage, gathering, and transfer

CONFIRM you have a comprehensive systems risk assessment in place that includes a full risk assessment by an impartial body.



Systems are in place to ensure communications between originating site and distant site are effective.

ASSESS the adequacy of bandwidth, quality of connection, and effectiveness of equipment used in the telehealth encounter.



Your organization's providers are appropriately credentialed and re-credentialed.

AUDIT your credentialing files to ensure all providers have appropriate credentialing documentation.



Appropriate support personnel capacity for each service line is in place.

ANALYZE provider and support capacity and resolve immediate capacity issues in a timely manner.



Patient consent is documented and includes the consultation of care via a virtual encounter.

CHECK a random sample of your patient files for patient consent documentation.



Technology proficiency training is provided to all providers involved in the delivery of telehealth services.

REVIEW plans for technology proficiency training for providers.



Developing and maintaining a patient-provider relationship in all telehealth encounters is a key priority.

INTERVIEW your staff regarding the process for promoting an appropriate patient-provider relationship.



All information regarding the encounter is documented.

AUDIT your patient files for full documentation of each encounter, including diagnosis, procedures, treatment, etc.



Each program is evaluated by analyzing and trending operational, clinical, and satisfaction performance indicators.

ANALYZE performance trends for performance indicators to evaluate the effectiveness of the program.