

etherFAX and HIPAA

The etherFAX solution is HIPAA compliant. It is also important to understand that there is no Federal Agency that 'certifies' that a solution is HIPAA Compliant. There are published guidelines that must be adhered to and the etherFAX solution does adhere to the HIPAA guidelines, which follow.

Technical Safeguards – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call back, and token systems.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.