HIPAA Compliance Matrix

WestFax goes beyond the normal technology assurances. We embed security policies and standard compliant practices in our everyday operations to guarantee the privacy, integrity, availability and accessibility of your electronic Protected Health Information (ePHI).

	Requirement Description	WestFax Assurance
Privacy Rule	Defines the covered entities and the other entities that may handle ePHI data. Business Associate (BA) requirements are defined. §164.305(a)	WestFax meets or exceeds the requirements of both the Security Rule and the Privacy rule. As a Business Associate we have the policies and procedures as well as the physical and technical security safeguards that guarantees your compliance.
Security Rule	Technical safeguards means the technology and the policy and procedures for its use that protect ePHI and control access to it. §164.304	WestFax addresses each area of concern with cutting edge technology and rock solid systems design. WestFax actively manages and audits its system to provide unsurpassed systems security and incident response. WestFax brings comprehensive compliance support that includes FISMA High / NIST SP 800-53, HIPAA, PCI-DSS Level 1, SOC 2 Type II, and SOC 3.
Physical Security	Providing the highest level of system security and reliability starts with securing the processing resources to prevent, unauthorized access, theft or destruction. § 164.312(a)(1)	WestFax systems are deployed in secure SOC 2 compliant data centers. 24×7 guard staff and Video/DVR surveillance of facility and server cages. ID and Authorization are required to enter building, with extra biometric control of “private cloud” areas. Strictly controlled, logged and audited third party access to the data centers.
Access Control	Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).	ePHI data is isolated to servers and storage system in the WestFax “private cloud” environment. Software and systems require user passwords.
Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity. §164.312(a)(2)	WestFax ensures the username is unique, and that each session providing access to data is authenticated. Password complexity policies are enforced to ensure that passwords cannot be guessed or compromised. WestFax user activity logging captures access and activity.
Automatic Log off	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. § 164.312(a)(2)(iii).	WestFax applications contain an idle timeout feature that will automatically log out users after a specified period of time. User access and permissions are reaffirmed every time the application is reopened. Applications are designed to prevent “remember me” features, removing risk of password compromise.
Person or Entity Authentication Control	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. §164.312(d)	Existing user login requires a username and password. Access to secure messages can be further protected by a multi-factor authentication and administrator controlled Access Control List (ACL).

	Requirement Description	WestFax Assurance
Transmission Security	Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network. § 164.312(e)(1)	The highest level of TLS encryption available for data in transit either through our secure website or secure API interfaces. WestFax supports TLS protected SMTP email with optional REQUIRE TLS extension in accordance with the IETF RFC 3207. FTPS and SFTP with TLS for safe and secure transport of documents to and from your existing servers.
Protection of ePHI at Rest	Encryption § 164.312(e)(2)(ii). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	WestFax assures the privacy of data while within our system by applying encryption at each phase of processing and through the use of Access Control Lists. At rest AES 256 bit encryption of ePHI data to guarantee privacy and prevent disclosure from intrusion. WestFax application architecture and file system security controls access for both external and internal system users accessing ePHI.
Data Integrity	Integrity means the that data or information have not been altered or destroyed in a manner that is not authorized. § 164.304	WestFax protects the integrity of electronic health information on its secure platform via end-to-end encryption and decryption of messages transferred over the TLS protocol. Signature protocol prevents data tampering while data is enroute. To protect against destruction, all messages are securely archived on a central server after encryption.
Data Availability	In addition to integrity, availability is that data is available for use at all times by authorized data recipients.	WestFax assures data availability by providing an online backup option for all data at rest. Redundant data centers and network paths provide always on data availability.
Audit Control	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. § 164.312(b)	Audit logs of external and internal system users are reviewed in real-time to proactively detect and prevent security issues. ID and Authorization is required to enter building, with extra biometric control of “private cloud” areas. Strictly controlled, logged and audited third party access to the data centers. 24×7 guard staff and Video/DVR surveillance of facility and server cages.