Can EFT help me comply with HIPAA rules?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT™ version 7 and later

QUESTION

Can EFT help me comply with HIPAA rules?

ANSWER

Yes, EFT can address the HIPAA **Technical Safeguards**. Other policies, procedures, or training require measures external to EFT, including the Administrative Safeguards and Physical Safeguards.

For a detailed HIPAA checklist, refer to IHS HIPAA Security Checklist. The Technical Safeguards are listed below.

HIPAA Security Rule	Safeguard	How EFT Addresses the Rule
164.312(a)(1)	**Access Controls:** 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	
164.312(a)(2)(i)	Have you assigned a unique name and/or number for identifying and tracking user identity?	EFT enforces unique usernames for users and administrators, provides granular administrative controls over user provisioning and authorization allows user and admin account revocation, provides automatic removal of inactive users after 90 days, includes controls for temporarily enabling/disabling users, auto-locks users after six failed login attempts either for a period of time or permanently until the admin

		unbans the IP address.
164.312(a)(2)(ii)	Have you established (and implemented as needed) procedures for obtaining for obtaining necessary EPHI during an emergency?	Requires measures external to EFT
164.312(a)(2)(iii)	Have you implemented procedures that terminate an electronic session after a predetermined time of inactivity?	EFT automatically expires session after a set period of inactivity
164.312(a)(2)(iv)	Have you implemented a mechanism to encrypt and decrypt EPHI?	Encrypt EPHI or other sensitive data using the EFT OpenPGP encryption module or third-party encryption utilities. Secure protocols such as SSL, TLS, and SFTP (SSH2) are provided for data transmission.
164.312(b)	Have you implemented Audit Controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI?	Reports of all activity (including administrator actions) within EFT can be generated on demand with the Auditing and Reporting Module. EFT will audit all user access to data, and all administrator changes to configuration settings. Access to audit trails, invalid logical access, authentication mechanisms, object creation, and initialization of audit log is managed at the database server. EFT audits user identity, type of transaction, date and time of transaction, transaction result, remote and local IP, and objects affected.
164.312(c)(1)	**Integrity:** Implement policies and procedures to protect	

	EPHI from improper alteration or destruction.	
164.312(c)(2)	Have you implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner?	The Content Integrity Control module is used in EFT Event Rules to send a file to an antivirus or data loss prevention scanner for processing. When this Action is added, a file that triggers the Event Rule is sent to an ICAP server for scanning. When the file passes the scan, other Actions can occur, such as moving the file to another location. If the file fails the scan, processing can stop, or other Actions can occur, such as sending an email notification.
164.312(d)	Have you implemented Person or Entity Authentication procedures to verify that a person or entity seeking access EPHI is the one claimed?	EFT supports various combinations of password, certificate, two-factor, and public-key authentication mechanisms, secures passwords during transmission (assumes SSL or SSH), and storage (with a one way [uniquely salted] hash), verifies identify before allowing password reset or lost username retrieval according to OWASP guidelines, includes minimum length and a number of complexity options, expires and forces password change after 90 days , disallows password re-use, internal dictionary match, or username match, and can

		force first time use password reset.
164.312(e)(1)	**Transmission Security:** Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Have you implemented security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of?	The Content Integrity Control module is used in EFT Event Rules to send a file to an antivirus or data loss prevention scanner for processing. When this Action is added, a file that triggers the Event Rule is sent to an ICAP server for scanning. When the file passes the scan, other Actions can occur, such as moving the file to another location. If the file fails the scan, processing can stop, or other Actions can occur, such as sending an email notification. The EFT Auditing and Reporting Module logs, tracks, and reports on all file transfers, access, admin activity, and user activity
164.312(e)(2)(ii)	Have you implemented a mechanism to encrypt EPHI whenever deemed appropriate?	EFT provides FIPS-compliant ciphers for encrypted transfers. Encrypt EPHI or other sensitive data using the EFT OpenPGP encryption module or third-party encryption utilities. Secure protocols such as SSL, TLS, and SFTP (SSH2) are provided for data transmission.

Can EFT help me comply with HIPAA rules?

.telerik-reTable-4 { border-collapse: collapse; border: solid 0px; font-family: Tahoma; } .telerik-reTable-4 tr.telerik-reTableHeaderRow-4 { border-width: 1.0pt 1.0pt 3.0pt 1.0pt; margin-top: 0in; margin-right: 0in; margin-bottom: 10.0pt; margin-left: 0in; line-height: 115%; font-size: 11.0pt; font-family: "Calibri" , "sans-serif"; background: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; color: #FFFFFF; } .telerik-reTable-4 td.telerik-reTableHeaderFirstCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderLastCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderOddCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableHeaderEvenCol-4 { padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 tr.telerik-reTableOddRow-4 { border-width: 1pt; color: #666666; vertical-align: top; border-bottom-style: solid; border-bottom-color: #4F81BD; } .telerik-reTable-4 tr.telerik-reTableEvenRow-4 { color: #666666; vertical-align: top; } .telerik-reTable-4 td.telerik-reTableFirstCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; border-left-style: solid; } .telerik-reTable-4 td.telerik-reTableLastCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-right-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableOddCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; } .telerik-reTable-4 td.telerik-reTableEvenCol-4 { border-width: 1pt; border-color: #4F81BD; padding: 0in 5.4pt 0in 5.4pt; border-bottom-style: solid; } .telerik-reTable-4 tr.telerik-reTableFooterRow-4 { color: #355C8C; background-color: #FFFFFF; vertical-align: top; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterFirstCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-left-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterLastCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; border-right-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterOddCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; padding: 0in 5.4pt 0in 5.4pt; } .telerik-reTable-4 td.telerik-reTableFooterEvenCol-4 { border-width: 1pt; border-color: #4F81BD; border-bottom-style: solid; padding: 0in 5.4pt 0in 5.4pt; }

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11382/Can-EFT-help-me-comply-with-...