Good and HIPAA

Provides the firewall, transmission, and handheld device security required by HIPAA's Security Rule

What is HIPAA?

The Health Insurance Portability & Accountability Act of 1996, also known as the Kennedy-Kassebaum Act, is designed to improve the safe portability of healthcare information across insurance carriers and healthcare providers through a standardization of data formats. The act also mandates privacy and security standards to protect patient information. Specifically, HIPAA:

- Improves the efficiency and portability of healthcare delivery by standardizing electronic data interchange, and
- Protects the confidentiality and security of patient healthcare information by enforcing standards for any organization that handles this information.

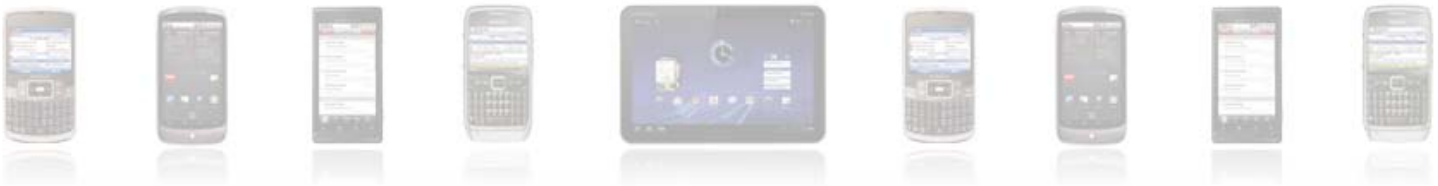
This document describes the features and capabilities that Good Technology provides to address the requirements of the HIPAA Security Rule.

Good Technology and HIPAA

Good Technology's connectivity, communication, and collaboration products are architected to align with the firewall, transmission, and smart-device security required by HIPAA's Security Rule. Full HIPAA compliance requires assessment of and potentially modification to the company's processes, policies, and procedures.

An example of Good's robust security architecture is Good for Enterprise—the email, contact management, and calendar component of the Good solution. Good for Enterprise uses cryptography-based security to protect sensitive information, and has achieved FIPS—Federal Information Processing—140-2 certification, which is based on a set of requirements by the U.S. Government.

Good™



Secure mobility that's compliant

The table below presents Good for Enterprise features that address various requirements of the HIPAA Security Rule.

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	Good for Enterprise Capabilities
ADMINISTRATIVE SAFEGUARDS			
Security Management Process	164.308(a)(1)	• Risk Analysis (R) • Risk Management (R) • Sanction Policy (R) • Information System Activity Review (R)	• N/A - policy/procedural requirement
Assigned Security Responsibility	164.308(a)(2)	(R)	• N/A - policy/procedural requirement
Workforce Security	164.308(a)(3)	• Authorization and/or Supervision (A) • Workforce Clearance Procedure • Termination Procedures (A)	• Bullets 1 & 2 - policy / procedural • Disable users via Good Mobile Control
Information Access Management	164.308(a)(4)	• Isolating Healthcare Clearinghouse Function (R) • Access Authorization (A) • Access Establishment & Modification (A)	• Rose-based-administration • Device password protection • Password policies (e.g. no repeat passwords allowed) • SSL / license key server authentication
Security Awareness and Training	164.308(a)(5)	• Security Reminders (A) • Protection from Malicious Software (A) • Log-in Monitoring (A) • Password Management (A)	• Device and application password protection • Time-based device locking
Security Incident Procedures	164.308(a)(6)	• Response and Reporting (R)	• Good Mobile Control allows continuous monitoring of device status • Remote erase of device data—or only enterprise data—allows control over device theft or loss incidents
Contingency Plan	164.308(a)(7)	• Backup Plan (R) • Disaster Recovery Plan (R) • Emergency Mode Operation Plan (R) • Testing & Revision Procedure (A) • Applications & Data Criticality Analysis (A)	• Data backup is a function of the Exchange or Domino server • Good Server standby / failover configuration capability
Evaluation	164.308(a)(8)	(R)	• N/A - policy/procedural requirement
Business Associate Contracts & Other Arrangement	164.308(b)(1)	• Written Contract or Other Arrangement (R)	• N/A - policy/procedural requirement
PHYSICAL SAFEGUARDS			
Facility Access Controls	164.310(a)(1)	•Contingency Operations (A) • Facility Security Plan (A) • Access Control & Validation Procedures (A) • Maintenance Records (A)	• Emails queuing when wireless network is down or device is not in coverage • Device password protection
Workstation Use	164.310(b)	(R)	• N/A - policy/procedural requirement
Workforce Security	164.310(c)	(R)	• Device password protection • Time-based device locking • Remote erase of device data, or only enterprise data
Device and Media Controls	164.310(d)(1)	• Disposal (R) • Media Re-use (R) • Accountability (A) • Data Backup and Storage (A)	• Remote erase of device data, or only enterprise data • Data backup is a function of the Exchange or Domino server
TECHNICAL SAFEGUARDS (SEE§164.312)			
Access Control	164.312(a)(1)	• Unique User Identification (R) • Emergency Access Procedure (R) • Automatic Logoff (A) • Encryption and Decryption (A)	• Device and application password protection • Device validation before emails are sent • Time-based device locking • AES encryption • FIPS 140-2 certification • Restrict unauthorized devices connection • Restrict unauthorized applications • In emergency, admin can recover user's password • Jailbroken/rooted device detection • Secure browser • SD card encryption
Audit Controls	164.312(b)	(R)	• Good audit trails of all emails sent to a device • Good Mobile Control allows continuous monitoring of device status
Integrity	164.312(c)(1)	• Mechanism to Authenticate Electronic Protected Health Information (A)	• Encryption / decryption provides integrity of data being transmitted
Authentication	164.312(d)	(R)	• Device or application password protection • Device validation before emails are sent • Disable cut, copy, and paste
Transmission Security	164.312(a)(1)	• Integrity Controls (A) • Encryption (A)	• AES encryption • FIPS 140-2 certification • No holes required in firewall

Appendix A to Subpart C of Part 164 – Security Standards: Matrix Columns 1-34 form the Federal Register, Vol. 68, No. 34

Good Technology
For more information visit www.good.com.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia/Pacific Headquarters
+61 (02) 92381953