



## WHAT IS HIPAA?

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

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

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

## GOOD TECHNOLOGY & HIPAA

Good Technology's robust wireless email and corporate data access products are designed to provide the firewall, transmission, and handheld device security required by HIPAA's Security Rule. While full HIPAA compliance requires assessment and potentially changes to processes, policies, and procedures, Good Technology provides the security features that — together with the appropriate policies and procedures — address HIPAA requirements.

As an example of our robust security architecture, Good Technology has achieved FIPS 140-2 certification. FIPS — Federal Information Processing Standards — are a set of requirements developed by the U.S. Government that govern how US federal agencies use cryptographic-based security systems to protect information in computer and telecommunication systems.

The table below shows security features that Good Technology provides to address the various requirements of the HIPAA Security Rule:

**Appendix A to Subpart C of Part 164—Security Standards: Matrix  
Columns 1-3 from the Federal Register, Vol. 68, No. 34**

<b>Standards</b>	<b>Sections</b>	<b>Implementation Specifications (R) = Required, (A) = Addressable</b>	<b>Good Technology Compliance</b>
<b>ADMINISTRATIVE SAFEGUARDS</b>			
Security Management Process	164.308(a)(1)	<ul style="list-style-type: none"> <li>• Risk Analysis (R)</li> <li>• Risk Management (R)</li> <li>• Sanction Policy (R)</li> <li>• Information System Activity Review (R)</li> </ul>	<ul style="list-style-type: none"> <li>• N/A – policy/procedural requirement</li> </ul>
Assigned Security Responsibility	164.308(a)(2)	(R)	<ul style="list-style-type: none"> <li>• N/A – policy/procedural requirement</li> </ul>
Workforce Security	164.308(a)(3)	<ul style="list-style-type: none"> <li>• Authorization and/or Supervision (A)</li> <li>• Workforce Clearance Procedure</li> <li>• Termination Procedures (A)</li> </ul>	<ul style="list-style-type: none"> <li>• Bullets 1 &amp; 2 - policy / procedural</li> <li>• Disable users via Good Management Console</li> </ul>
Information Access Management	164.308(a)(4)	<ul style="list-style-type: none"> <li>• Isolating healthcare Clearinghouse Function (R)</li> <li>• Access Authorization (A)</li> <li>• Access Establishment &amp; Modification (A)</li> </ul>	<ul style="list-style-type: none"> <li>• Role-based-administration</li> <li>• Device password protection</li> <li>• Password policies (e.g. no repeat passwords allowed)</li> <li>• SSL / license key server authentication</li> </ul>
Security Awareness and Training	164.308(a)(5)	<ul style="list-style-type: none"> <li>• Security Reminders (A)</li> <li>• Protection from Malicious Software (A)</li> <li>• Log-in Monitoring (A)</li> <li>• Password Management (A)</li> </ul>	<ul style="list-style-type: none"> <li>• Device password protection</li> <li>• Time based device locking</li> <li>• Virtual private network minimizes malicious software intrusion</li> </ul>
Security Incident Procedures	164.308(a)(6)	<ul style="list-style-type: none"> <li>• Response and Reporting (R)</li> </ul>	<ul style="list-style-type: none"> <li>• Good Monitoring Portal allows continuous monitoring of device status</li> <li>• Remote erase of device data allows control over device theft or loss incidents</li> </ul>
Contingency Plan	164.308(a)(7)	<ul style="list-style-type: none"> <li>• Backup Plan (R)</li> <li>• Disaster Recovery Plan (R)</li> <li>• Emergency Mode Operation Plan (R)</li> <li>• Testing &amp; Revision Procedure (A)</li> <li>• Applications &amp; Data Criticality Analysis (A)</li> </ul>	<ul style="list-style-type: none"> <li>• Handheld backup to memory card</li> <li>• Data backup is a function of the Exchange server</li> <li>• Good Server standby / failover configuration capability</li> </ul>
Evaluation	164.308(a)(8)	(R)	<ul style="list-style-type: none"> <li>• N/A – policy/procedural requirement</li> </ul>
Business Associate Contracts & Other Arrangement	164.308(b)(1)	<ul style="list-style-type: none"> <li>• Written Contract or Other Arrangement (R)</li> </ul>	<ul style="list-style-type: none"> <li>• N/A – policy/procedural requirement</li> </ul>

Appendix A to Subpart C of Part 164—Security Standards: Matrix  
Continued

Standards	Sections	Implementation Specifications (R) = Required, (A) = Addressable	Good Technology Compliance
<b>PHYSICAL SAFEGUARDS</b>			
Facility Access Controls	164.310(a)(1)	<ul style="list-style-type: none"> <li>Contingency Operations (A)</li> <li>Facility Security Plan (A)</li> <li>Access Control and Validation Procedures (A)</li> <li>Maintenance Records (A)</li> </ul>	<ul style="list-style-type: none"> <li>Emails queuing when wireless network is down or device is not in coverage</li> <li>Device password protection</li> </ul>
Workstation Use	164.310(b)	(R)	<ul style="list-style-type: none"> <li>N/A – policy/procedural requirement</li> </ul>
Workstation Security	164.310(c)	(R)	<ul style="list-style-type: none"> <li>Device password protection</li> <li>Time based device locking</li> <li>Remote erase of device data</li> </ul>
Device and Media Controls	164.310(d)(1)	<ul style="list-style-type: none"> <li>Disposal (R)</li> <li>Media Re-use (R)</li> <li>Accountability (A)</li> <li>Data Backup and Storage (A)</li> </ul>	<ul style="list-style-type: none"> <li>Remote erase of device data</li> <li>Data backup is a function of the Exchange server</li> </ul>
<b>TECHNICAL SAFEGUARDS (SEE § 164.312)</b>			
Access Control	164.312(a)(1)	<ul style="list-style-type: none"> <li>Unique User Identification (R)</li> <li>Emergency Access Procedure (R)</li> <li>Automatic Logoff (A)</li> <li>Encryption and Decryption (A)</li> </ul>	<ul style="list-style-type: none"> <li>Device password protection</li> <li>Device validation before emails are sent</li> <li>Time based device locking</li> <li>AES encryption</li> <li>FIPS 140-2 certification</li> </ul>
Audit Controls	164.312(b)	(R)	<ul style="list-style-type: none"> <li>Good audit trails of all emails sent to a device</li> <li>Good Monitoring Portal allows continuous monitoring of device status</li> </ul>
Integrity	164.312(c)(1)	<ul style="list-style-type: none"> <li>Mechanism to Authenticate Electronic Protected Health Information (A)</li> </ul>	<ul style="list-style-type: none"> <li>Encryption / decryption provides integrity of data being transmitted</li> </ul>
Person or Entity Authentication	164.312(d)	(R)	<ul style="list-style-type: none"> <li>Device password protection</li> <li>Device validation before emails are sent</li> </ul>
Transmission Security	164.312(e)(1)	<ul style="list-style-type: none"> <li>Integrity Controls (A)</li> <li>Encryption (A)</li> </ul>	<ul style="list-style-type: none"> <li>AES encryption</li> <li>FIPS 140-2 certification</li> <li>No holes required in firewall</li> </ul>

**Good Technology, Inc.**

For more information, please call 866.BE.GOOD or visit [www.good.com](http://www.good.com)

©2004 Good Technology, Inc. All rights reserved. Good, the Good Logo, GoodLink, GoodAccess and “Good for Business. Great for You.” are trademarks or registered trademarks of Good Technology, Inc. in the United States and/or other countries. All other trademarks are property of their respective holders. Good Technology, Inc. and its products and services are not related to, sponsored by, or affiliated with Research In Motion Limited.

