

MGBE HIPAA Policy Reference Guide

Topic	Policy
Appropriate Access	<ul style="list-style-type: none"> • Confidentiality Agreement • IT Access Control Security Policy (EISP-9) • IT Access Control Standards for Users (EISS-9b)
Cloud Services	<ul style="list-style-type: none"> • Enterprise IT Asset Management Policy (EISP-8) • IT Asset Management Standards for Acceptable Use (EISS-8a)
Corrective Action	<ul style="list-style-type: none"> • Managing Workforce Members Information Security Responsibilities Policy (EISP-7) • Policy for Sanctions Addressing Information Security and Privacy Violations (EISP-7b)
Data Classification	<ul style="list-style-type: none"> • IT Asset Management Standards for Data Classification (EISS-8c)
Email	<ul style="list-style-type: none"> • E-mail Security Policy • IT Asset Management Standards for Acceptable Use of ITRs (EISS-8a) • Requests to Receive Unencrypted Email
Fax	<ul style="list-style-type: none"> • Safeguarding Fax Copiers Printers Telephone Use and Pagers (PH-145)
Firewalls	<ul style="list-style-type: none"> • IT Access Control Standards for Networks (EISS-9a)
Mail	<ul style="list-style-type: none"> • Patient and Research Subject Mailings
Mobile Device Security (Encryption)	<ul style="list-style-type: none"> • Enterprise IT Asset Management Policy (EISP-8) • IT Asset Management Standards for Apple Macintosh Products (EISS 8d)
Text Messaging	<ul style="list-style-type: none"> • Obtaining Consent to Text Patients and Research Subjects PH-157
Patching and Antivirus	<ul style="list-style-type: none"> • IT Acquisition, SDLC and Maintenance Policy (EISP-12)
Password Security	<ul style="list-style-type: none"> • IT Access Control Security Policy (EISP-9) • IT Access Control Standards for Users (EISS-9b) • IT Asset Management Standards for Acceptable Use of ITRs (EISS-8a)
Physical Removal and Transport	<ul style="list-style-type: none"> • Physical Removal and Transport of Protected Health Information and Personal Information (PH-155)
Physical Security (Piggy-Backing)	<ul style="list-style-type: none"> • Physical Security and Environmental Controls for Electronic Information Policy (EISP-11)

Principles of Privacy	<ul style="list-style-type: none"> • Minimum Necessary Standard (PH-112)
Protected Health Information	<ul style="list-style-type: none"> • Definition of Protected Health Information (PHI)
Records and Information Management Policy	<ul style="list-style-type: none"> • Mass General Brigham Records and Information Management Policy
Reporting Information Security and Privacy Incidents	<ul style="list-style-type: none"> • Information Security and Privacy Incident Response Policy (EISP-16) • Internal Reporting Procedures (ISPR-16a)
Risk Assessments	<ul style="list-style-type: none"> • Enterprise IT Asset Management Policy (EISP-8)
Secure Disposal	<ul style="list-style-type: none"> • Secure Media Destruction Procedures (ISPR-8a)
Sharing Information	<ul style="list-style-type: none"> • Obtaining Authorization for Release of PHI (PH-123) • Use and Disclosure of PHI (PH-102)
Social Media, Videos Photography, and Other Recordings	<ul style="list-style-type: none"> • IT Asset Management Standards for Acceptable Use of ITRs (EISS-8a) • Partners HealthCare Social Media Policy • Photography and Audio Video Recording of Patients for Clinical Purposes (PH-156)
Treatment, Payment, and Operations (TPO)	<ul style="list-style-type: none"> • Definition of TPO
Workforce Responsibility to Protect PHI	<ul style="list-style-type: none"> • Information Security and Privacy Training (PH-109) • Information Security Program Policy (EISP-5) • Managing Workforce Members Information Security Responsibilities Policy (EISP-7)
Workstation Security	<ul style="list-style-type: none"> • IT Access Control Security Policy (EISP-9)