MGMA®
MEDICAL GROUP
MANAGEMENT
ASSOCIATION

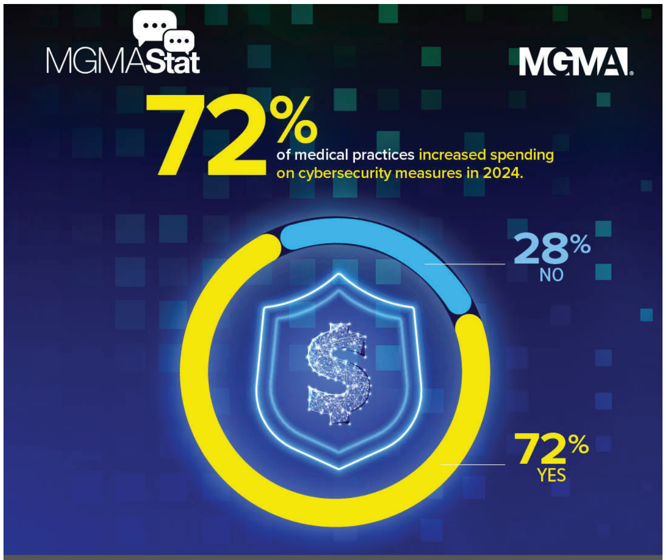
playbook

Cybersecurity in Medical Practices

The price of security paid, in prevention or recovery

Healthcare organizations are always feeling the heat when it comes to protecting sensitive data. According to **a 2023 report by IBM**, the healthcare industry experienced the highest average cost of a data breach for the 13th consecutive year, with an average of $10.93 million per breach.

A September 2024 MGMA *Stat* **poll** found that more than seven in 10 (72%) medical group practices increased their spending on cybersecurity measures in 2024, while 28% did not. The most common sources of these rising expenses? Cybersecurity insurance, more threats and risks to the organization, and implementation of additional security measures, infrastructure updates and employee training.



MGMA *Stat* poll. September 17, 2024 | Has your org increased spending on cybersecurity measures in 2024? 326 responses. MGMA.COM/STAT, #MGMASTAT

In the spirit of recognizing that cybersecurity issues as a matter of "when," not "if" — plus the exceptional regulatory framework in place to ensure the safeguarding of protected health information (PHI) — this playbook is designed to lay out the foundations of HIPAA compliance and cybersecurity requirements, as well as how-to approaches and best practices around staff training, access control, network and physical security, and securing EHRs, PM systems and vendor platforms.

TABLE OF CONTENTS

HIPAA compliance and cybersecurity requirements

Healthcare is one of the most targeted industries across the globe for cyberattacks, and the HIPAA Security and Privacy rules play key roles in the standards and safeguards used today to protect the growing, interconnected systems and devices used by hospitals, medical groups and the rest of the care delivery ecosystem.

In particular, **the Security Rule** specifically sets out to ensure the "confidentiality, integrity, and security" of electronic protected health information (ePHI). What does that mean?

- **Confidentiality:** ePHI is not available or disclosed to unauthorized persons.
- **Integrity:** ePHI is not altered or destroyed in an unauthorized manner.
- **Availability:** ePHI is accessible and usable on demand by an authorized person.

> **"The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.**
>
> **The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information."**
>
> **45 CFR Parts 160, 162, and 164**

Key HIPAA Security Rule components

- **Appoint a security officer**: Assign someone responsible for overseeing HIPAA security compliance, which includes managing risk assessments, audits and staff training.
- **Implement access controls**: Limit access to ePHI to authorized personnel only, and use strong password policies, multi-factor authentication (MFA) and user role-based access.
- **Conduct regular risk assessments**: These are explicitly required for HIPAA compliance. Covered entities and business associates are required to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI)." This is often referred to as a "risk assessment" or "risk analysis."
  - A one-time risk assessment is not enough. Risk assessments need to be **ongoing** and **periodic** to ensure that new threats, vulnerabilities and changes to systems are consistently evaluated. This should be annually or as dictated by your organization's risk profile.
  - Document all risk assessment processes and results to meet HIPAA audit requirements.
- **Schedule regular security audits**: While a risk assessment identifies threats and vulnerabilities, **security audits** go deeper into validating whether your safeguards and controls are both in place and effective.
  - **Administrative safeguards**: Audits check for proper security policies, workforce training, and contingency planning.
  - **Physical safeguards**: Audits assess physical controls around facility access and device security.
  - **Technical safeguards**: Audits evaluate technical controls such as encryption, access controls and network monitoring.
  - By conducting these audits on a **scheduled basis** (e.g., annually or quarterly, depending on the organization's size and risk profile), you can detect and address any areas of non-compliance before they become liabilities.
- **Establish data backup systems**: Regularly back up ePHI and store backups securely offsite.
- **Enable audit logs**: Activate and monitor audit logs for all systems handling ePHI.

NIST Cybersecurity Framework (CSF)
for guidelines on robust access control strategies

HIPAA Security Risk Assessment Tool
from HealthIT.gov

MGMA HIPAA Medical Practice Compliance Fillable Form Book

HHS-OCR Contingency Planning/Data Backup Guidance

HHS-OCR HIPAA Audit Controls Guidance

Staff training, access control and authentication

By integrating these best practices and action steps, healthcare organizations can establish a robust framework to safeguard sensitive systems, comply with regulatory requirements, and build a culture of cybersecurity awareness.

Training to identify phishing emails and scams

Phishing remains a top cybersecurity threat in healthcare. Effective training helps staff recognize and respond to suspicious activities.

BEST PRACTICES

- **Interactive modules**: Incorporate real-world phishing examples into training materials.
- **Visual cues**: Teach staff to identify red flags like misspelled URLs, urgent language, and unexpected attachments.
- **Incident reporting**: Establish a clear protocol for reporting suspicious emails.

ACTION STEPS

1. Schedule annual training sessions focusing on evolving phishing tactics.
2. Provide quick-reference guides for staff, highlighting common phishing indicators.
3. Conduct follow-up assessments to reinforce knowledge retention.

Simulated drills for staff readiness

Simulated phishing attacks are invaluable for gauging preparedness and identifying gaps in awareness.

BEST PRACTICES

- **Tailored scenarios**: Use email templates that mimic realistic threats faced by healthcare staff.
- **Immediate feedback**: Provide instant feedback when staff fail simulations, highlighting learning points.
- **Gamification**: Reward teams or individuals for high performance to encourage engagement.

ACTION STEPS

1. Launch quarterly or randomized phishing simulations, varying complexity based on staff roles.
2. Track participation and success rates, creating individual improvement plans where needed.
3. Integrate drill results into broader cybersecurity awareness initiatives.

Least privilege principles to restrict access

The principle of least privilege ensures that users only have access to the resources necessary for their roles.

BEST PRACTICES

- **Role-based access control (RBAC)**: Define and assign access levels based on job functions.
- **Periodic audits**: Regularly review access permissions to remove unnecessary privileges.
- **Automated alerts**: Deploy systems to flag attempts to access restricted data.

ACTION STEPS

1. Develop a role-specific matrix detailing access levels.
2. Schedule quarterly access reviews, adjusting permissions as needed.
3. Utilize software tools to enforce and monitor least privilege policies.

continued on next page »

Staff training, access control and authentication

» continued from previous page

Periodic password update requirements with complexity rules

Strong, regularly updated passwords help mitigate brute-force and credential-stuffing attacks.

BEST PRACTICES

- **Complexity standards**: Enforce minimum requirements (e.g., length, alphanumeric, special characters).
- **Change intervals**: Require password changes every 60–90 days.
- **No reuse**: Prohibit the reuse of recent passwords.

Monitoring for and addressing unauthorized access attempts

Continuous monitoring helps detect and mitigate breaches before they escalate.

BEST PRACTICES

- **Real-time alerts**: Set up notifications for failed login attempts or unusual access patterns.
- **Logging and analysis**: Maintain detailed access logs for forensic analysis.
- **Proactive response plans**: Define actions for addressing unauthorized access attempts.

ACTION STEPS

1. Deploy security information and event management (SIEM) tools.
2. Train IT teams to analyze access logs and respond promptly to anomalies.
3. Conduct periodic reviews to refine monitoring protocols.

Network and physical security essentials

Firewalls and intrusion detection systems (IDS)

- Deploy next-generation firewalls (NGFWs) to monitor and filter traffic based on applications and threats.
- Use intrusion detection/prevention systems (IDS/IPS) to identify and block malicious activity.
- Regularly update firewall and IDS/IPS rules to address emerging threats.
- Conduct periodic reviews of logs and reports for suspicious activity.

Router and switch security configuration

- Change default credentials and disable unused ports and protocols.
- Enable secure management protocols like SSH and disable Telnet.
- Apply firmware updates and patches regularly.
- Use access control lists (ACLs) to limit traffic based on source and destination.

Additional Resources:

NIST Guidelines on Firewalls and Firewall Policy

NIST Guide to Intrusion Detection and Prevention Systems

NIST Guidelines for Securing Wireless Local Area Networks

Securing WiFi networks with encryption, segmentation

- Configure Wi-Fi with WPA3 encryption for maximum security.
- Use network segmentation to isolate guest Wi-Fi and critical systems.
- Disable broadcasting of unnecessary SSIDs and restrict access with strong passwords.
- Periodically audit connected devices and access policies.

Monitoring network traffic for suspicious activity

- Implement network monitoring tools (e.g., SIEM) to analyze traffic patterns in real-time.
- Use AI-driven analytics to detect anomalies and unusual behaviors.
- Set up alerts for unusual bandwidth usage or unauthorized access attempts.
- Regularly review traffic logs to identify and address vulnerabilities.

continued on next page »

Network and physical security essentials

» continued from previous page

Vulnerability scans and penetration tests

- Schedule regular vulnerability scans to identify and mitigate weaknesses. For larger organizations, do this monthly.
- Conduct annual or semi-annual penetration tests using internal or external experts.
- Prioritize and remediate findings based on risk severity.
- Document and review test results to improve the organization's security posture.

Securing server rooms with access control systems

- Use keycard or biometric access control systems to restrict entry.
- Maintain a log of all access attempts and review regularly.
- Limit physical access to authorized personnel only.
- Conduct periodic audits to ensure compliance with access policies.

Surveillance systems for critical IT infrastructure areas

- Install high-definition surveillance cameras in server rooms and critical areas.
- Integrate motion detection and alerts to enhance monitoring.
- Retain footage for a minimum of 30 days for investigative purposes.
- Regularly test and maintain camera systems to ensure functionality.

Locking down physical access to workstations, devices

- Equip workstations with cable locks or secure mounting hardware.
- Use proximity cards or PIN locks to restrict access to shared devices.
- Implement auto-lock settings for unattended devices after a short idle period.
- Educate staff on safeguarding devices against unauthorized access.

Implementing environmental controls

- Maintain optimal temperature (64–80°F) and humidity levels (40–60%) in server rooms.
- Install uninterruptible power supplies (UPS) to prevent downtime during outages.
- Deploy fire suppression systems and ensure proper ventilation.
- Regularly inspect and maintain HVAC systems to avoid environmental hazards.

Additional Resources:

NIST Security and Privacy Controls
Covering technical controls, including secure configuration management for network devices

NIST Technical Guide to Information Security Testing and Assessment

HIPAA Security Rule - Physcial Safeguards

NIST Physical and Environmental (PE) Controls

Securing EHR and PM systems

Access controls for user roles

- Implement role-based access controls (RBAC) to ensure users only access data necessary for their roles.
- Regularly review and adjust user permissions, especially after role changes.
- Require individual logins to track activity accurately and prevent shared access.

Regular updates and patches

- Enable automatic updates or establish a patch management schedule to apply vendor-released updates promptly.
- Test updates in a controlled environment before deployment to avoid system disruptions.
- Monitor vendor alerts for critical vulnerabilities and prioritize urgent fixes.

Secure workstations and limit EHR access

- Require strong passwords and multi-factor authentication (MFA) for workstation and system access.
- Configure automatic logout or lockout after periods of inactivity.
- Physically secure workstations in locked offices or with cable locks in shared spaces.

Audits of EHR access logs

- Perform routine audits of access logs to identify unauthorized or unusual access patterns.
- Use automated tools to flag suspicious activity, such as access to large volumes of records.
- Maintain a documented process for investigating and resolving access violations.

Encrypting patient data during storage and transmission

- Use Advanced Encryption Standard (AES) for data at rest and Transport Layer Security (TLS) for data in transit.
- Employ full-disk encryption for devices storing EHR data.
- Periodically review encryption protocols to ensure compliance with industry standards.

Device and endpoint security

Mobile device management (MDM)

- Enforce MDM solutions to monitor, manage, and secure mobile devices accessing organizational data.
- Require device enrollment in MDM before accessing healthcare systems.
- Enable remote wipe capabilities for lost or stolen devices.
- Restrict installation of unauthorized apps and enforce strong passcodes.

Encrypting portable devices

- Use full-disk encryption (e.g., BitLocker, FileVault) on laptops.
- Deploy hardware-encrypted USB drives for data transfer.
- Prohibit storing sensitive data on unencrypted external devices.
- Periodically audit devices for encryption compliance.

Secure disposal of outdated devices

- Use certified data destruction services for hard drives and electronic components.
  Ensure they follow NIST SP 800-88 guidelines for secure data destruction or media sanitization.
- Overwrite or physically destroy storage media before disposal.
- Maintain a disposal log to document compliance with regulatory standards.
- Verify secure data removal before donating or recycling devices.

Configuring automatic software updates and training staff

- Enable automatic updates for operating systems, security patches, and applications. Centralize update management for organizational devices using endpoint management tools.
- Regularly review and update device settings to address new vulnerabilities.
- Test critical updates before deployment to avoid compatibility issues.
- Educate staff on secure remote access practices, including using virtual private networks (VPNs) and MFA.
- Require training completion to obtain system access.
- Provide clear guidelines on device security, such as avoiding public Wi-Fi and ensuring device encryption.

Data backup and recovery planning

Creating an automated, redundant backup system

- Implement automated daily backups for critical systems and data. Ensure that all backup systems meet HIPAA requirements for encryption and access control both in transit and at rest.
- Use redundant systems (on-site and off-site) to ensure data availability.
- Regularly verify backup integrity to avoid corrupted or incomplete backups.

Testing recovery plans for disaster scenarios

- Conduct quarterly recovery drills simulating various disaster scenarios.
- Test for recovery time objectives (RTO) and recovery point objectives (RPO) compliance.
- Document lessons learned and refine recovery protocols after each test.

Choosing between on-site, cloud, or hybrid backup strategies

- Evaluate organizational needs and budget to decide between on-site, cloud, or hybrid systems.
- Hybrid backups offer flexibility, with cloud ensuring off-site safety and on-site enabling fast recovery.
- Ensure cloud providers comply with HIPAA and maintain robust security measures.

Compliance with HIPAA backup requirements

- Ensure backups include all ePHI.
- Encrypt backups in transit and at rest to protect patient data.
- Maintain access controls and a disaster recovery plan in line with HIPAA requirements.

Documenting the recovery process to minimize downtime

- Develop a detailed recovery plan outlining roles, steps, and timelines for data restoration.
- Keep documentation accessible to authorized personnel during emergencies.
- Review and update the recovery plan annually or after significant changes in systems.

Additional Resources:

NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise

MGMA Member Tool: Planning and Deployment of a Mobile Device Management System

HHS - Proper Disposal of Electronic Devices for guidelines on robust access control strategies

HIPAA Security Rule - Device and Media Controls

HHS - Data Backup Plan Guidance

NIST Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities

HHS - Guidance on HIPAA & Cloud Computing

HIPAA Security Rule - Backup & Disaster Recovery

MGMA *Stat*: Averting crisis with a well-documented plan for EHR, RCM downtime

Incident response and breach management

Incident response plans and downtime protocols

- Develop and maintain a detailed incident response plan outlining detection, containment, recovery, and communication steps.
- Include downtime protocols to ensure continuity of critical operations, such as reverting to manual processes.
- Test the plan annually with simulated incidents and refine based on outcomes.
- Maintain a hardcopy incident response playbook accessible during system downtimes.

Steps to contain and mitigate damage of a cyberattack

- Immediately isolate affected systems to prevent further spread.
- Block compromised accounts and change credentials organization-wide.
- Identify and address vulnerabilities that allowed the breach (e.g., patching, removing malware).
- Monitor systems closely for residual threats or suspicious activity.

Roles and responsibilities during a breach

- Assign clear roles, including an Incident Response Lead, IT/security teams, legal advisors, and communication liaisons.
- Provide staff with contact lists and escalation protocols for emergencies.
- Train all team members on their responsibilities as part of the response process.

Legal requirements for breach notifications to patients and regulators

- Follow HIPAA's 60-day notification rule for breaches involving 500+ patients. For breaches involving fewer than 500 individuals, report to HHS within 60 days of the end of the calendar year.
- Notify individuals, HHS, and possibly the media, depending on breach scope. Specifically, notify the media if the breach affects more than 500 individuals in a single state or jurisdiction.
- Include detailed information in notifications: nature of the breach, affected data, response actions, and steps for individuals to protect themselves.
- Document all notifications and response actions to ensure compliance.

Additional Resources:

MGMA Member Tool: Incident Response Plan Checklist

HIPAA Breach Notification Rule (45 CFR §§ 164.400-414)

OCR - Breach Portal ("Wall of Shame")

HHS Guidance on Risk Assessment & Breach Notification

Vendor security

Vetting vendors for cybersecurity practices and compliance

- Conduct detailed assessments of vendors' security policies, including compliance with HIPAA and other relevant standards.
- Require vendors to complete security questionnaires and provide evidence of certifications like SOC 2 or HITRUST. Ensure certifications align with the organization's security priorities and applicable regulatory requirements.
- Prioritize vendors with proven track records in healthcare cybersecurity.

Drafting strong data security agreements in vendor contracts

- Include detailed provisions for data encryption, access controls, and breach notification timelines.
- Require vendors to indemnify the organization against breaches caused by their negligence.
- Specify regular audit rights and security reporting obligations.

Monitoring vendors' access to sensitive data

- Limit vendor access to only the data and systems necessary for their role.
- Use activity logging to monitor and audit vendor interactions with sensitive information.
- Revoke access immediately when vendor contracts end or roles change.

Creating contingency plans in case of vendor-related breaches

- Integrate vendor-specific scenarios into the organization's incident response plan.
- Ensure vendors have their own breach response processes and align them with organizational protocols.
- Maintain backup systems and alternative vendors to ensure business continuity.

Periodic review of vendor compliance and security certifications

- Conduct annual reviews of vendor compliance, including updated certifications and security audits, as well as reviews of BAAs.
- Require regular security updates and documentation of their systems and practices.
- Terminate contracts with vendors that fail to meet agreed-upon security standards.

Additional Resources:

MGMA Business Associate Agreement Outline

HHS HIPAA BAA Guidance

HHS Sample BAA Provisions

HITRUST Alliance Developer of a common security framework and certification program used by many healthcare vendors

Resources

RECOMMENDATIONS IN THIS PLAYBOOK

- Incident Response Plan Checklist
- Risk & Compliance Toolkit
- MGMA HIPAA Medical Practice Compliance Fillable Form Book
- Planning and Deployment of a Mobile Device Management System
- Business Associate Agreement Outline

ADDITIONAL TOOLS AND PERSPECTIVES

- HIPAA for Professionals
- Summary of the HIPAA Security Rule
- The HIPAA Privacy Rule
- OCR Cybersecurity Guidance Materials

playbook

MGMA Playbooks collect MGMA's best data, tools and resources to help you solve your problems and prepare for future sustainability and growth. Playbooks are currently for MEMBERS ONLY.

To discuss your membership or benefits, contact
MGMA Customer Service Team at 877.275.6462 ext. 1888
or **service@mgma.com**

See also **mgma.com/membership**

Inspiring
healthcare
excellence.SM

MGMA®