All In Remote Physician Academy

HIPAA Compliance and Data Security Quick Reference

HIPAA Compliance and Data Security Quick Reference

Summary of Security Requirements & Best Practices

Encryption Requirements

Encryption is essential for protecting sensitive data from unauthorized access.

Key requirements include:

- Data at Rest: Encrypt stored patient data using AES-256 encryption.
- Data in Transit: Use TLS 1.2 or higher for securing data transfers.
- Email Encryption: Implement secure email protocols such as S/MIME or PGP.
- Device Encryption: Ensure all company laptops and mobile devices have full-disk encryption enabled.
- Backup Encryption: Securely encrypt all data backups with access controls.
- Access Controls: Enforce strict access policies to prevent unauthorized data decryption.

Multi-Factor Authentication (MFA) Setup

MFA adds an extra layer of security by requiring multiple forms of verification.

Steps for setting up MFA:

- Enable MFA for all accounts handling patient data and administrative tasks.
- Choose an Authentication Method:
  - Authenticator app (Google Authenticator, Microsoft Authenticator)
  - SMS or email codes (less secure than app-based authentication)
  - Hardware tokens (YubiKey, RSA SecurID)
- Implement Role-Based Access Control (RBAC):
  - Limit administrative access to only necessary personnel.
  - Require higher security levels for privileged accounts.
- Regularly Review and Update MFA Policies:
  - Require periodic re-authentication.
  - Ensure MFA is mandatory for remote access.

HIPAA Compliance and Data Security Quick Reference

Summary of Security Requirements & Best Practices

Firewall Recommendations

Firewalls are crucial for safeguarding networks against unauthorized access and cyber threats.

Best practices include:

- Deploy Network Firewalls: Use enterprise-grade firewalls with intrusion detection and prevention.
- Enable Application-Level Filtering: Block unauthorized applications from accessing sensitive data.
- Implement VPN for Remote Access: Ensure secure connections for remote employees.
- Regularly Update Firewall Rules: Conduct periodic audits to refine security policies.
- Segment Networks: Isolate sensitive patient data from general IT infrastructure.
- Monitor Traffic Logs: Enable real-time monitoring for suspicious activity

Patient Confidentiality Tips

Ensuring privacy in both digital and physical spaces is essential for compliance and trust.
Key strategies include:

Physical Privacy

- Soundproofing: Use noise-canceling technology or soundproofing panels in consultation areas.
- Secure Conference Rooms: Restrict access to rooms where sensitive conversations occur.
- Privacy Screens: Install screen filters on monitors to prevent unauthorized viewing.
- Controlled Access Areas: Use keycard or biometric entry systems for restricted zones.

Digital Privacy

- Screen Timeout Policies: Set screens to lock automatically after periods of inactivity.
- Restricted Device Use: Prohibit unauthorized devices from connecting to the network.
- Encrypted Messaging: Use HIPAA-compliant platforms for patient communication.
- Regular Training: Educate staff on best practices for handling confidential information.