HIPAA Security Best Practices

Practical security measures for healthcare organizations

Password Policies

- [ ] Minimum 12 characters with complexity requirements
- [ ] Password expiration every 90 days
- [ ] No password reuse for last 12 passwords
- [ ] Multi-factor authentication (MFA) required
- [ ] Account lockout after 5 failed attempts

Encryption Standards

- [ ] AES-256 encryption for data at rest
- [ ] TLS 1.2 or higher for data in transit
- [ ] Full disk encryption on all devices
- [ ] Encrypted backups stored securely
- [ ] Email encryption for PHI communications

Access Management

- [ ] Principle of least privilege enforced
- [ ] Regular access reviews (quarterly)
- [ ] Immediate access revocation upon termination
- [ ] Separate admin and user accounts
- [ ] Privileged access management (PAM) system

Incident Response Planning

- [ ] Written incident response plan
- [ ] Designated incident response team
- [ ] 24/7 incident reporting hotline
- [ ] Breach notification procedures (60-day timeline)
- [ ] Annual incident response drills
- [ ] Post-incident review process

Employee Training

- [ ] HIPAA training for all employees within 30 days of hire
- [ ]

- [ ] Annual refresher training
- [ ] Role-specific security training
- [ ] Phishing awareness training
- [ ] Training documentation and tracking

Physical Security

- [ ] Controlled facility access
- [ ] Visitor logs and badges
- [ ] Secure disposal of PHI (shredding, wiping)
- [ ] Workstation security (privacy screens, auto-lock)
- [ ] Surveillance cameras in sensitive areas