Security Compliance Best Practices

Ensure your organization has adequate controls in place to protect confidential member information

We are dedicated to protecting confidential information about our members. As our trusted business partner, we need your help in this important effort. Please review the following best practices to ensure you have adequate controls in place.

Administrative Safeguards

- Documented compliance program to address requirements of the Health Insurance Portability and Accountability Act (HIPAA)
- Written policies and procedures addressing HIPAA privacy, security and breach notification requirements
- Designated compliance, privacy and/or security officer
- Employee and agent/subcontractor background checks upon hire
- Periodic risk assessments performed by an independent third party to test internal controls for protecting confidential information

Agreements

- Confidentiality agreements for all employees, agents and subcontractors who access confidential member information
- Business associate agreements with third parties who access protected health information (PHI)

Training

- Annual all employee compliance training that contains privacy/security awareness and describes how to report issues of non-compliance and HIPAA disclosures
- Training should be documented and include sanctions for non-completion

Physical Safeguards

- Facility access controls, including keycard requirements
- Workstation use and security controls
- Device and media controls
- Physical access controls to servers, network equipment and physical documents

MEDICAL MUTUAL®

Technical Safeguards

Network security

- Network boundaries are protected by firewalls
- Regular network vulnerability scans and penetration tests are performed
- Intrusion detection systems (IDS) or intrusion prevention systems (IPS) are used
- Employees must use a virtual private network (VPN) to access system from all remote locations
- Encryption is used when emailing confidential information

Systems security

- Computer systems (servers) are backed up regularly
- Audit logs are maintained for system access
- Malware, virus and phishing protection is in place that includes monitoring threats 24/7
- Established, documented procedures are in place for patching against vulnerabilities
- All security events are logged, monitored, reviewed, reported and followed up on until resolved

Device security

- Written policy and procedure governing portable devices and removable media
- All devices containing confidential data must be encrypted

Access controls

- Employee and agent/subcontractor access is reviewed and recertified at least once per year
- Access to confidential information is restricted to employees or agents/subcontractors who require access to perform essential work duties
- Permitted uses and disclosures of PHI are limited to the minimum necessary information to achieve the purpose for which PHI is disclosed
- Access permissions are removed promptly when employees, agents and subcontractors are terminated or resign
- Controls in place to ensure PHI cannot be altered or destroyed in an unauthorized manner
- Audit logs are used to review and monitor access

Passwords

- Written policies restricting the sharing of credentials for internal or third-party systems/applications
- Unique user IDs and passwords are required to identify/authenticate each user
- Written password policy that ensures strong password rules are enforced (e.g., minimum eight characters, includes numbers, symbols, and a mix of different types of characters, passwords cannot be reused, are not visible on screens, are stored in an encrypted format)

Incident Response

- Documented and published process informing employees how to report any suspected or actual HIPAA violations with an option to report anonymously
- Policies against retaliation for good faith reporting
- Formal, documented and tested plan that addresses the organization's response to a cybersecurity event (updated and tested regularly)
- Cybersecurity insurance with appropriate limits based on the amount of records maintained
- Corrective action policy to address violations

Data Retention

- Documented governance for secure disposal, transfer, removal and reuse of PHI (physical and electronic)
- Client confidential information deleted or shredded when it is no longer needed
- Hardcopy media shredded/destroyed when no longer needed
- Procedures established for the cleaning of the hard drive when a device is retired

Disaster Recovery and Business Continuity Plan

- Business continuity plan is in place and updated periodically
- Existence of a recovery site
- Annual disaster recovery simulation testing