HIPAA and HITECH Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

ABC Company values its relationships with our health care customers, service providers, and regulators. Managing compliance requirements helps us maximize our opportunities in the market, enhances our competitive position, and helps build trust.

# II. Purpose

The Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and Canadian Personal Health Information Protection Act (PHIPA) specify security standards, privacy requirements, and security breach notification procedures. A strong health care compliance program provides our organization with a competitive advantage, helps protect our image and reputation, and reduces our costs.

# III. Scope

This policy applies to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

# IV. Policy

HIPAA is designed to protect sensitive health care information through improved security standards and privacy legislation. It defines requirements for collecting, storing, and transmitting patient information. It also identifies compliance guidelines for critical business tasks such as risk analysis, awareness training, audit trail, disaster recovery plans, information access, and encryption.

HITECH requires entities, business associates, vendors of personal health records and related entities to notify individuals when their personal health information is subject to a breach of security. To limit exposure, limited data sets with de-identified data shall be used to disclose only the minimum necessary protected health information.

To meet compliance requirements, ABC Company shall implement the required information security standards as outlined in the HIPAA Security Rule. The security standards are organized into three major safeguard areas:

* Administrative Safeguards - policies and procedures for day-to-day operations, managing the conduct of employees with access to electronic protected health information (EPHI) as well as managing the selection, development, and use of security controls.
* Physical Safeguards - security measures that protect an organization's electronic information systems, buildings, and equipment from natural hazards, environmental hazards, and unauthorized intrusion.
* Technical Safeguards - security measures that specify how to use technology to protect electronically protected health information and access to such information.

The table below identifies ABC Company policies and plans that implement and maintain specific Safeguards to meet HIPAA, HITECH, and PHIPA compliance requirements. While larger firms generally have a designated Chief Privacy Officer (CPO), smaller organizations may have a Chief Security Official (CSO) fulfill these duties. For more information on Business Associates, refer to the Third Party Service Providers Policy.

|  |  |  |
| --- | --- | --- |
| **Security Control** | **Policy and Plan** | **Health** |
| Governance | IT Governance Policy  Mergers and Acquisitions Policy  Terms and Definitions Policy | 164.308 |
| Information Security | Privacy Policy  Securing Information Systems Policy  Security Controls Review Policy | 422.112 |
| Risk Management | Business Impact Analysis  Risk Assessment Policy  Risk Management Policy | 45 CFR 164.308  422.504  820.22 |
| Policies and Procedures | Security Policy  Security Policy Intro  System Security Plan | 422.112  422.202 |
| Organization | Audit Policy  IT Governance Policy  IT Management Policy  IT Support Staffing Policy  Outsourcing Policy | 422.503  ARRA 13408  13404(b)  13405(b) |
| Asset Management | Data Classification Policy  Network Access Policy  Software Licensing Policy | 21 CFR  11.1(b)  11.1(f) |
| Human Resources | Acceptable Use Policy  Security Awareness & Training Plan  Security Awareness & Training Policy  Staffing Policy  Social Networking Security Policy  Third Party Service Providers Policy | 21 CFR  820.20b  820.75b  820.25a  PHIPA |
| Physical and Environmental | Personnel Security Policy  Physical Access Security Policy  Physical Security Policy | 164.310 |
| Communications and Operations | Account Management Policy  Anti-Malware Policy  Backup Policy  Bluetooth Policy  Data Integrity Policy  Data Marking Policy  Data Privacy Policy  Domain Controller Policy  Domain Name System Policy  E-commerce Policy  Electronic Disposal Policy  E-mail Policy  Firewall Policy  Guess Access Policy  Internet Connection Policy  Intrusion Detection Policy  Logging Policy  Mass Communication Policy  Network Address Policy  Network Configuration Policy  Network Documentation Policy  Removable Media Policy  Router Security Policy  Security Monitoring Policy  Server Hardening Policy  Vendor Access Policy  Workstation Security Policy | 820-60  820-65 |
| Access Control | Admin Special Access Policy  Asset Management Policy  Bring Your Own Device Policy  Guest Access Policy  Identification and Authentication  Logical Access Controls Policy  Network Access Policy  Password Policy  Mobile Device Policy  Remote Access Policy  Securing Information Systems Policy  Securing Sensitive Information Policy  Smartphone Policy  System Update Policy  User Privilege Policy  Web Policy  Wireless Access Policy | 422.501  495.346  21 CFR  11.1e  11.10d  11.10k |
| Acquisition Development and Maintenance | Acquisition and Procurement Policy  Application Implementation Policy  Approved Application Policy  Audit Trails Policy  Change Management Policy  Encryption Policy  Green Computing Policy  Hardware and Software Maintenance  Patch Management Policy  Production Input Output Controls  Quality Assurance Policy  Secure Development Lifecycle Policy  Server Certificates Policy  Software Development Policy  VPN Policy  Web Site Policy | 495.348  820.50  820.80 |
| Incident Management | Identity Theft Protection Policy  Incident Response Policy  Incident Response Plan  Reporting Violations Policy | 422.128  ARRA  13402 |
| Business Continuity Management | Business Continuity Plan  Business Continuity Policy  Business Resumption Plan  Continuity Communications Plan  Dept Continuity of Operations Plan  IS Disaster Recovery Plan  Resilience Policy | 164.308 |
| Compliance | Certification and Accreditation Policy  Compliance Policy  Electronic Data Retention Policy  HIPAA and HITECH Policy | ARRA  13405(a) |

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who have access to or manage Information Resources that collect, transmit, process, or store health care related data.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO09.05, APO12.02, APO13.07, DSS04.05, MEA03.01, MEA04.11

GDPR Article 25, 32

HIPAA 164.308, 164.310, 164.312, 164.314, 164.316, 164.502, ARRA 13402, 13404, 13405

ISO 27001:2013 6.1.2, A5, A7.2.2, A8.1.3, A8.2.1, A9-14, A16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8