Time Doctor

HIPAA Compliance Policies and Procedures

Purpose

The purpose of this policy is to establish requirements for the proper handling of protected health information (PHI) through the adoption of an information privacy and security management process for Time Doctor. Such a process is required as a means of managing the privacy and security of PHI under the HIPAA Privacy Rule, the HIPAA Security Rule §164.308(a)(1), to comply with any other applicable information security regulations, and to protect the overall security of the organization.

The process includes the analysis and management of risks, the implementation of secure systems and applications, the use of security incident procedures to learn from prior issues, information system usage audits and activity reviews, regular security evaluations and regulation compliance assessments, training for all staff using electronic information systems, and documentation of compliance activities.

This policy defines the technical controls and security configurations that users and information technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Time Doctor. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within Time Doctor with policies and guidelines concerning the acceptable use of Time Doctor technology equipment, email, internet connections, voicemail, future technology resources, and information processing.

Scope

This policy document defines common security requirements for all Time Doctor personnel and systems that create, maintain, store, access, process, or transmit information. This policy also applies to information resources owned by others, such as contractors of Time Doctor, entities in the private sector, and cases where Time Doctor has a legal, contractual, or fiduciary duty to protect said resources while in Time Doctor custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Time Doctor network system which consists of various hardware, software, communication equipment, and other devices designed to assist Time Doctor in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Time Doctor domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by Time Doctor at its office locations or at remote locales.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, slides, models, wireless, telecommunication, conversations, servers, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Time Doctor employees or temporary workers at all locations and by contractors working with Time Doctor as subcontractors.

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

Time Doctor

HIPAA Compliance Policies and Procedures

Policy

Time Doctor shall establish procedures to create and maintain an information security management process to ensure the confidentiality, integrity, and availability of protected health information (PHI), other personal and private information as required by law or regulations, and essential business information. The policy and procedures include the following sections:

1.1. Assigned Privacy and Security Responsibility
1.2. HIPAA Privacy Rule Compliance
1.3. Risk Assessment, Risk Analysis, and Risk Management
1.4. Information Security and Compliance Evaluation
1.5. Implementation of Secure Systems and Applications
1.6. Information System Usage Audits and Activity Reviews
1.7. Backup and Disaster Recovery
1.8. Information Security Incidents
1.9. Training
1.10. Sanctions for Policy Violations
1.11. Documentation

1.1 Assigned Privacy and Security Responsibility

§164.530(a) of the HIPAA Privacy Rule and §164.308(a)(2) of the HIPAA Security Rule each require the designation of a single individual with the responsibility for the development and implementation of the policies and procedures required for compliance. Time Doctor will assign the security officer responsibility for all matters relating to the safeguarding of the privacy and security of personal or private information to the chief technology officer (CTO). The security officer may delegate activities to the information security team (IST). This individual or team (as appropriate) will be responsible for ensuring that all personal or private information is protected against reasonably anticipated threats or hazards to the security and integrity of the information and against reasonably anticipated improper uses.

The HIPAA security officer will be the initial point of contact in any security compliance inquiry.

The HIPAA security officer will have oversight for:

a. Ensuring that all policies and procedures required under applicable standards and regulations are established and maintained over time.

b. Monitoring the appropriate and consistent implementation of policies and procedures.

c. Ensuring that all members of the workforce, contractors, and business associates are aware of and abide by the policies and procedures.

d. Monitoring and analyzing security alerts and information and ensuring proper follow-up action.

e. The investigation of information security incidents and/or breaches.

f. The administration of user accounts, including additions, deletions, and modifications, and monitoring and controlling all access to data.

g. Ensuring that any security weaknesses discovered in the course of security incidents or security evaluations will be prioritized for correction and corrected.

h. Ensuring that the analyses and documentation required by applicable standards and regulations, and/or Timedoctor's security policies and procedures, are carried out fully and completely.

The HIPAA privacy officer will be responsible for receiving any complaints about HIPAA compliance and will be the initial point of contact in any privacy compliance inquiry.

1.2 HIPAA Privacy Rule Compliance

Time Doctor and its staff shall treat all PHI as confidential information and only access the minimum necessary to perform their job functions. PHI shall not be used or disclosed in any way other than as indicated in the business associate agreements as agreed to by Time Doctor.

In the event that Time Doctor does retain and manage data that is considered to be part of a patient's designated record set in a medical record, Time Doctor will develop policies and procedures to satisfy the individual rights defined in the HIPAA Privacy Rule § 164.520-528 as necessary and appropriate.

In the event of any improper disclosures in violation of the HIPAA Privacy Rule, steps will be taken to limit and mitigate any harmful effects of such disclosures per §164.530(f).

The policy on training and documentation for compliance with the HIPAA Privacy Rule is integrated with that for compliance with the HIPAA Security Rule and the HIPAA Breach Notification Rule.

1.3 Risk Assessment, Risk Analysis, and Risk Management

Time Doctor shall regularly, at least annually, evaluate its information security-related policies and procedures to ensure that they meet the requirements of the HIPAA Security Rule and HIPAA Breach Notification Rule (§164.300et seq.and §164.400et seq.). A compliance evaluation shall also be required whenever there is a change in environmental or operational conditions that may affect the security of PHI.

Risks shall be mitigated and managed by Time Doctor to the best of its abilities, within reasonable and appropriate constraints of cost, staff ability, and hardware and software capabilities, according to a regularly developed and updated risk management plan based on the risk analysis.

The risk analysis and assessment shall be reviewed and updated whenever there are material changes in systems or operations controlled by Time Doctor or significant changes in the security environment in which Time Doctor operates, no less frequently than once every year.

1.4 Information Security and Compliance Evaluation

Time Doctor shall develop procedures to establish regular, periodic evaluations of the information security-related technical measures, policies, and procedures in place at the organization to ensure that they continue to meet the requirements of HIPAA Security Rule §164.308(a)(8). The period of review shall be at least annual and determined according to the organization's information systems risk analysis and its consideration of best practices. Evaluations shall be documented for regulatory compliance and to provide direction to the organization in the execution of its security management process and plans.

1.5 Implementation of Secure Systems and Applications

It is the policy of Time Doctor to implement and maintain systems and applications using secure best practices, whether developed in-house or procured from an external vendor. Procedures shall be developed to address:

- Documentation requirements;
- Default passwords and parameters;
- Password suppression and account lockout;
- Automatic logoff;
- Wireless access;
- Configuration standards;
- Administrative access;
- Patch management;
- Vulnerability management;
- Software development practices;
- Change control;
- Platform security;
- Web-based software and applications;
- Application security;
- Application backup and restoration; and
- Security configurations for desktop and laptop computers.

Time Doctor shall have procedures to track changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information (ePHI). Change tracking allows the information technology (IT) department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other changes to the system.

1.6 Information System Usage Audits and Activity Reviews

Time Doctor implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information (ePHI). Audit controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

Time Doctor shall establish a process for conducting, on a periodic basis, at least annually, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Time Doctor shall conduct an internal review of records of system activity on a regular basis to minimize security violations.

1.7 Backup and Disaster Recovery

It is the policy of Time Doctor to prepare for contingencies and ensure an appropriate response to emergencies or other occurrences that may damage systems that contain electronic confidential information, such as protected health information (PHI), and maintain usable copies of electronically held confidential information for use in such responses, if appropriate, as required by HIPAA Security Rule §164.308(a)(7) and by other applicable state or federal regulations. Information not required to be maintained shall be disposed of according to the defined procedures.

Contingency plans must take into account the criticality of applications/systems and data and the effects of short-term interruptions (such as brief power or system failures) and long-term disruptions (such as a loss of facilities or an epidemic).

Procedures shall be established that are sufficient to restore lost or damaged data with a useful duplicate, including the definition of which file systems to back up, the frequency of backups and media rotation, off-site storage requirements, the documentation and labeling of storage media, and the regular testing of backed-up data to ensure adequacy.

Backup and restoration procedures for electronic media and information systems containing critical data must be tested according to the frequency and practices as established in the individual system backup plans.

Time Doctor management shall maintain a detailed disaster recovery policy (DRP). This plan addresses the hardware and software configurations and detailed recovery procedures. Plans

and procedures shall be sufficient to ensure the restoration of lost data and system access, including a full range of information and activities needed to assure that the plan and its implementation will be effective.

1.8 Information Security Incidents

Time Doctor shall have in place an information security incident response policy, including procedures for the reporting, processing, and response to suspected or known information security incidents in order to investigate, mitigate, and document such incidents so that security violations may be reported and handled promptly, using an orderly process known to all workforce members, according to the HIPAA Breach Notification Rule and the HIPAA Security Rule §164.308(a)(6).

1.9 Training

Time Doctor shall establish an information privacy and security awareness and training program for the purpose of ensuring that all workforce members, including management, are aware of the organization's security policies and procedures and general principles of information security, as required by the HIPAA Privacy Rule and the HIPAA Security Rule §164.308(a)(5). Training must be provided to new staff before access to PHI is permitted and must be provided to all staff at least annually. Procedures shall include a definition of when training is to occur, for whom, and what training content, documentation, and acknowledgment will be provided.

1.10 Sanctions for Policy Violations

As appropriate, any member of the workforce who does not comply with the security policies and procedures of Time Doctor or who otherwise misuses or misappropriates personal or private information will be subject to disciplinary action according to the organization's disciplinary procedures. Workforce members in violation of security policies and procedures may be subject to:

1. A verbal warning;
2. A notice of disciplinary action placed in personnel files;
3. The removal of system privileges;
4. Termination of employment and/or contract penalties;
5. Civil or criminal penalties which may include notifying law enforcement officials, regulatory accreditation, and licensure organizations; or
6. Other sanctions as identified in the organization's disciplinary procedures.

1.11 Documentation

Time Doctor shall document any policies and procedures implemented under the requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, the HIPAA Breach Notification Rule, and other applicable information security regulations. Time Doctor shall also document any actions, activities, and assessments required to be performed under applicable HIPAA regulations under the requirements of the policies enacted in support of such regulations.