GATEKEEPER

GATEKEEPER HIPAA COMPLIANCE GUIDE

PURPOSE

This document was developed to provide Untethered Labs, Inc. a resource for the Health Insurance Portability and Accountability Act (HIPAA) tailored to the GateKeeper Platform. For customers that must comply with HIPAA it is imperative that they and their systems, to include the GateKeeper platform, meet all applicable security controls as outlined within this document.

BACKGROUND

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the development of regulations to protect the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

- **The Privacy Rule**, or Standards for Privacy of Individually Identifiable Health Information, establishes standards for the protection of certain health information.
- **The Security Rule**, or Security Standards for the Protection of Electronic Protected Health Information, establishes security standards for protecting certain health information that is held or transferred in electronic form.

HIPAA PRIVACY RULE

The HIPAA Privacy Rule sets national standards for the protection of individually identifiable health information by three types of "covered entities": health plans, health care clearinghouses, and health care providers who conduct the standard health care transactions electronically.

HIPAA SECURITY RULE

The HIPAA Security Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI).

1) Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit
2) Identify and protect against reasonably anticipated threats to the security or integrity of the information
3) Protect against reasonably anticipated, impermissible uses or disclosures
4) Ensure compliance by their workforce

ADMINISTRATIVE SAFEGUARDS

Security Management Process - A covered entity must identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.

Security Personnel - A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

Information Access Management - Consistent with the Privacy Rule standard limiting uses and disclosures of PHI to the "minimum necessary," the Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role (role-based access).

Workforce Training and Management - A covered entity must provide for appropriate authorization and supervision of workforce members who work with e-PHI. A covered entity must train all workforce members regarding its security policies and procedures, and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

Evaluation - A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

PHYSICAL SAFEGUARDS

Facility Access and Control - A covered entity must limit physical access to its facilities while ensuring that authorized access is allowed.

Workstation and Device Security - A covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity also must have in place policies and procedures regarding the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of electronic protected health information (e-PHI).

TECHNICAL SAFEGUARDS

Access Control - A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Audit Controls - A covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.

Integrity Controls - A covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

Transmission Security - A covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.

GateKeeper HIPAA Compliance Reference Card

Health Insurance Portability and Accountability Act (HIPAA) provides for the protection of individually identifiable health information that is transmitted or maintained in any form or medium. The privacy and security rules affect the day-to-day business operations of health care providers, health plans, health care clearing houses and other similar organizations. This document describes how GateKeeper can be an effective tool to help address security requirements as part of the customer's HIPAA compliance program.

Section	Key Activity	Performance Criteria	GateKeeper Solution
164.306(b)	Flexibility of Approach	(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.	GateKeeper increases the security, and decreases the complexity of the covered entity by providing an automatic mechanism for the locking of a workstation when a user is no longer in proximity. A user does not have to manually lock their workstation when they are no longer present. This security mechanism decreases the potential risks to ePHI.
164.308(a)(5)(ii)(C)	Security Awareness, Training, and Tools -- Log-in Monitoring	Procedures for monitoring log-in attempts and reporting discrepancies.	GateKeeper enterprise provides auditing and monitoring of all login events.
164.310(c)	Workstation Security	Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	GateKeeper provides a mechanism to automatically prevent unauthorized access to unattended computers.
164.312(a)(2)(i)	Access Control -- Unique User Identification	Assign a unique name and/or number for identifying and tracking user identity.	Each GateKeeper token serial number is associated with a user identity. Users can be identified and tracked by the hardware dongle identifier.
164.312(a)(2)(iii)	Access Control -- Automatic Logoff	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Combined with an organization's group policy for automatic logoff, GateKeeper provides an additional layer of access control by automatically locking a workstation when a user is no longer in proximity.
164.312(b)	Audit Controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	GateKeeper audits user login activity within the enterprise platform.
164.312(d)	Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	GateKeeper uses a hardware token associated with an active directory account to create a multi-factor authentication system.

GATEKEEPER
gkaccess.com

Untethered Labs, Inc., 5000 College Avenue, Suite 2103, College Park, MD 20740
Sales: 240-547-5446 • Visit us at gkaccess.com