

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	<p>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.</p> <p>In deciding which security measures to use, a covered entity or business associate must take into account the following factors:</p> <ul style="list-style-type: none"> ○ The size, complexity, and capabilities of the covered entity or business associate. ○ The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. ○ The costs of security measures. ○ 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.