PORTALGUARD

HIPAA Compliance Toolkit

Tech Brief

v.3.2-001

PistolStar, Inc. dba PortalGuard
PO Box 1226
Amherst, NH 03031 USA

Phone: 603.547.1200
E-mail: sales@portalguard.com
Website: www.portalguard.com

NIST 800-66 HIPAA Compliance

Health Insurance Portability and Accountability Act—Title II

If you are a healthcare provider and are navigating the tricky world of HIPAA Title II Compliance we can help. The PortalGuard authentication platform can help you meet a number of HIPAA's Title II security related requirements quickly, efficiently and cost effectively.

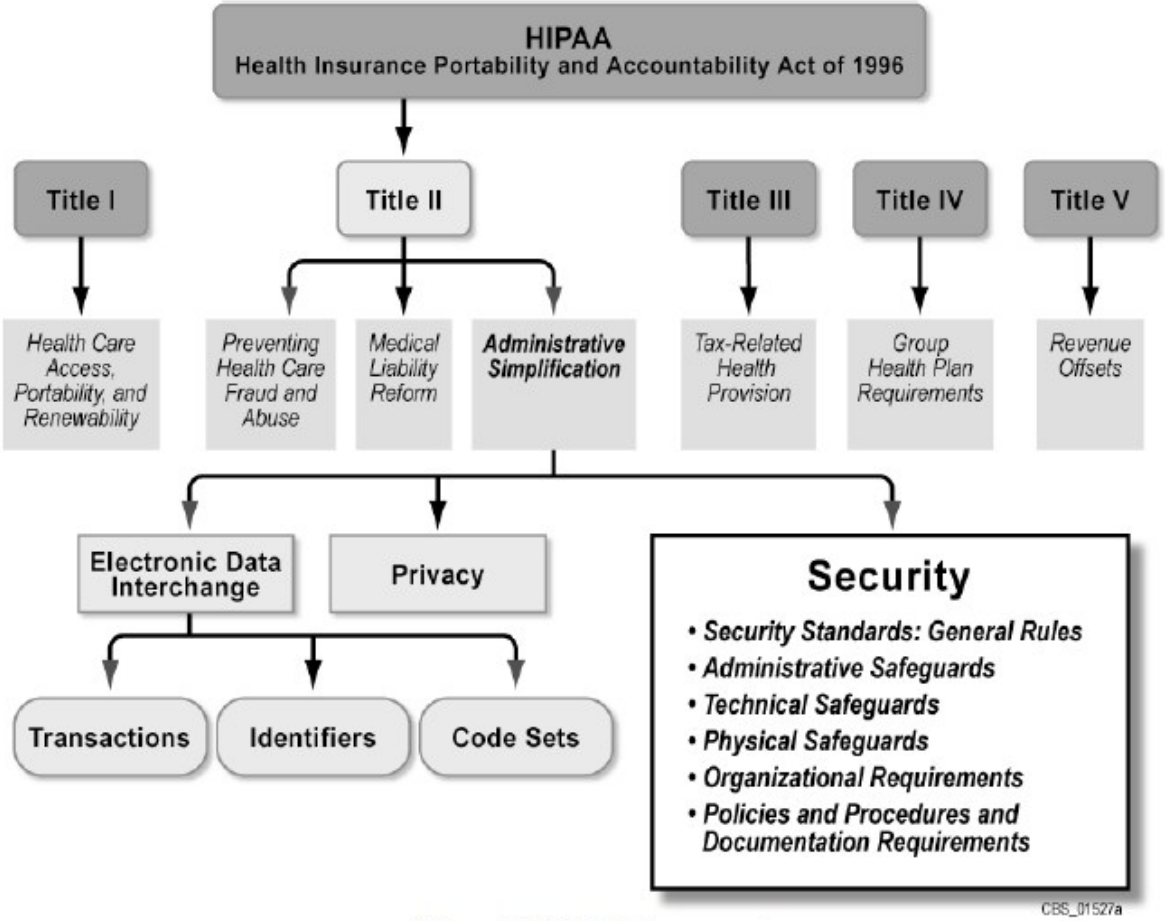

Figure 1. HIPAA Components

PortalGuard Compliance Matrix

The attached matrix summarizes the components of compliance that PortalGuard can help you address. Whether you're preparing for an audit, answering existing compliance issues or implementing a new system call us today and we'd be happy to discuss how our platform can help.

Control No.	Key Activity	Description	PortalGuard Feature
Technical Safeguards (4.14.8)	Automatic Logoff	Implement electronic procedures that terminate a session after a predetermined time of inactivity	PortalGuard is fully configurable to automatically logoff users after “x” amount of inactivity time.
Audit Controls (4.15.1)	Audit/Track Activities	Maintain audit records for specific events (e.g. User ID, time, location, date, time, etc.)	PortalGuard offers the ability to track user logins by ID, location, time, date, duration along with failed login attempts using our dashboard.
Integrity (4.16.1)	Identify All Users with Authorized Access	Identify all users with the ability to access, alter, or destroy data.	PortalGuard ties into your organizations MS Active Directory to give you complete control over system access either by individual or user group.
Integrity (4.16.3/4)	Develop & Implement Integrity Policy	Establish a formal procedure on system access and implement the methods used to support system integrity.	Our platform of applications provide the framework for a strong authentication policy to be written on. Fully customizable based on user ID and location.
Authentication (4.17.1)	Implement Mechanism to authenticate ePHI	Authentication requires establishing the validity of a transmission source and/ or verifying an individual’s claim that he/she is authorized to access the systems.	Full two-factor authorization that relies on both a password (something they know) and either laptop, desktop or mobile phone (something they have) for user authentication.
Transmission Security (4.18.2/3)	Implement Integrity Controls	Implement security measures to ensure that electronically transmit ePHI is properly executed.	PortalGuard can be configured to deny access if certain risk criteria are present (e.g. login from an unsecured public WiFi)