COLORTOKENS

MEETING HIPAA COMPLIANCE

WITH COLORTOKENS XTENDED ZEROTRUST PLATFORM

TECHNICAL BRIEF

Introduction

ColorTokens helps healthcare organizations meet their HIPAA guidelines, limit the scope of their audits, and accelerate the remediation of failed audits. The ColorTokens Xtended ZeroTrust™ Platform, based on a zero trust architecture, can see, stop, and predict security and compliance violations across any workload, any application, any deployment, and any user. Through a unified approach, healthcare organizations can simplify security and compliance across their entire IT environment. ColorTokens is the only vendor that can, in a single unified platform, protect an organization's backend servers, cloud servers, endpoints, and healthcare operations down to each process on every machine. This document serves as a summary reference on the mapping of HIPAA guidelines (v3.2.1) as well as some common challenges and attacks that HIPAA regulated entities can overcome with ColorTokens.

HIPAA Specific Challenges

HIPAA compliance in healthcare can be enormously challenging for a multi-story and multi-building campus that has hundreds and thousands of connected medical devices. A large number of Wi-Fi zones and RF environments in connected hospitals pose significant security challenges. ColorTokens can help to simplify and accelerate HIPAA compliance in the following critical areas:

Protect ePHI data: Doctors, nurses and other hospital staff, including contractors, constantly access electronic protected health Information (ePHI) to provide effective and real-time care to patients. Inside a hospital environment, there are very few ways to restrict who can see what data, leaving ePHI vulnerable and IT teams unaware about who is accessing what information, and why it is being accessed. ColorTokens provides a comprehensive asset inventory of resources by storing, processing and transmitting ePHI. Security operators can see all incoming and outgoing traffic across critical assets and healthcare information system (HIS) applications – providing security teams with confidence in the security and compliance posture of the organization.

Risk analysis and management: The high value of medical data is driving up the number of cyber attacks in the healthcare industry. To protect the ePHI database, HIS applications, and sensitive data, security teams need to understand the risks associated with these critical assets. ColorTokens provides the real-time contextual view into cybersecurity risk that helps to identify security policy needs. ColorTokens provides automated security policy recommendations to accelerate the HIPAA compliance journey. Users are also provided with a holistic risk view of their critical assets through integration with vulnerability management tools.

Simplify and limit scope of an audit: HIPAA audits can be costly. Failure of an audit can be expensive in terms of escalating fines, reputational damage and loss of trust from patients. In addition, the cost of the audit can be an enormous expense in itself, and the cost increases if the scope is not well defined. The ColorTokens visualizer simplifies defining the overall scope of the environment, by providing a holistic view into network flows and capabilities that enforce granular segmentation and isolation of ePHI assets from the rest of the environment.

ColorTokens can provide auditors with reports and interactive views to understand in minutes how hospitals are approaching effective data segmentation for protecting patient records and medical data.

Attack Vectors in Healthcare Environments

ColorTokens helps to ensure that HIPAA regulated healthcare providers not only achieve compliance but also maintain a strong security posture by avoiding common attack vectors. Many of the breaches that have occurred in healthcare have happened through a few common points of entry:

Healthcare Malware: Targeted phishing emails to healthcare staff and contractors are being used as an entry point to initiate stealthy advanced persistent attacks. ColorTokens can isolate segments with critical medical records and block the attack at the initial attack surface.

Insider Attacks: The abundance of insider attacks launched by disgruntled employees, lack of cyber hygiene and family snooping has been rising. To combat this, ColorTokens can help segment users, application environments and data that can be accessed. This provides granular security control and ensures that only legitimate users have access to the authorized information.

Point of Sale (POS) Terminals: The lack of visibility into the inventory of assets and the configuration of a POS (for e.g., enabling encryption or preventing employees from accessing the Internet through these terminals) can increase the likelihood of an attack. ColorTokens addresses this vulnerability with its policy-based encryption, endpoint lockdown capabilities, and holistic visibility of assets across the organization.

HIPAA Mapping to the ColorTokens Xtended ZeroTrust™ Platform

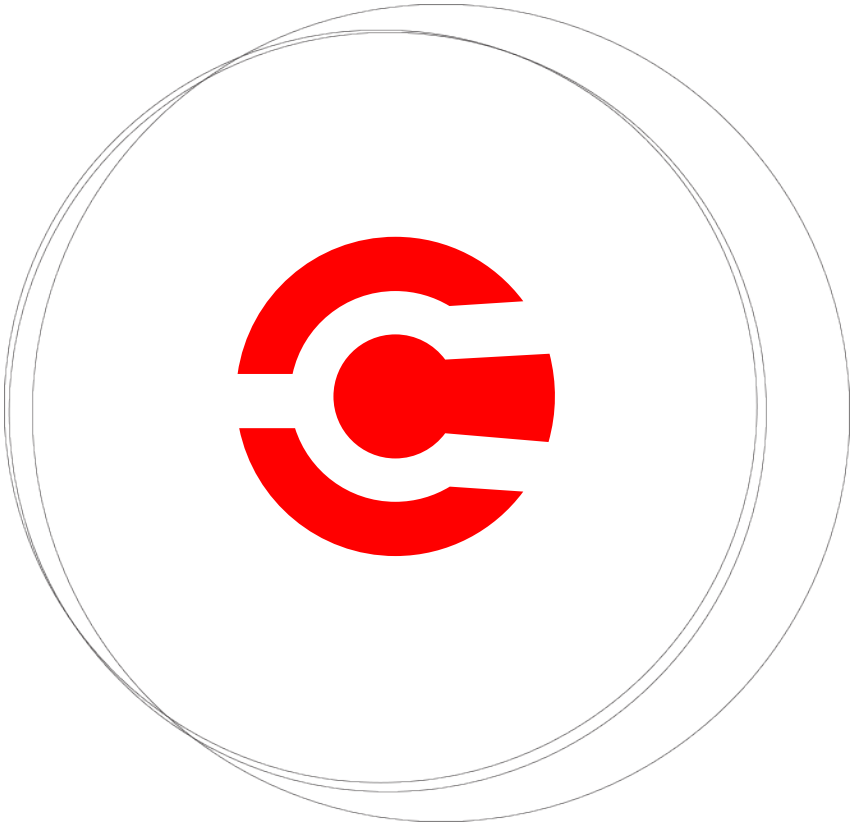
The ColorTokens zero trust security platform provides supporting evidence to an auditor, administrator, or an executive on how ColorTokens ensures the protection of sensitive data and compliance. As this is a high-level summary, we encourage readers to contact ColorTokens for an extensive review of the platform's complete HIPAA compliance and audit response capabilities. Please use the following checklist to identify your organization's level of HIPAA compliance.

Table 1 HIPAA Compliance using ColorTokens Xtended ZeroTrust Security Platform

HIPAA Requirement	Sub Requirements Addressed by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
Administrative Safeguards		
Security Management Process	164.308(a)(1) - 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(D)	• Eliminate blind spots with comprehensive visibility to traffic flows. • Map your application flows, vulnerabilities and user access to get comprehensive view to cyber risk • Enforce Zero Trust security architecture to significantly reduce attack surface and exposure of vulnerabilities. • Use real-time visualizer to know cyber risk by discovering policy non-compliances, unauthorized traffic flows and malicious processes. • Faster investigation with historical data sets and response to any security incidences with speed and accuracy.
Workforce Security	164.308(a)(3) - 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C)	• Visualize the current state of user access to healthcare applications. • Enforce policies to access healthcare applications based on the roles and responsibilities. • Users can be provided access to part of application functions (Web, App, DB) based on operations they should perform. • Visualizer provides real-time view to user to application traffic flows for administrative supervision. • Historical traffic flow is stored for later analysis. • User access can be revoked based on the business requirements.
Information Access Management	164.308(a)(4) - 164.308(a)(4)(ii)(A) 164.308(a)(4)(ii)(B (a)(4)(ii)(C)	• Application centric segmentation to isolate healthcare applications from rest of the environments. • Access to applications based on network, user identity and service. • Simplified compliance assurance with real-time view to application security state.
Security Awareness and Training	164.308(a)(5) - 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C)	• Allows only approved applications to run on workstations. • Signature-less technology with out-of-box integrated threat intelligence to detect malicious softwares and prevents their execution.

Technical Safeguards		
Access Control	164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(iii) 164.312(a)(2)(iv)	• Provision to create unique user accounts (ID) and provide access to applications. • User are logged-out after 30 minutes of idle time. • Encryption is supported to secure data flows between users to application and application to application.
Audit Controls	164.312(b)	• All network logs are recorded to have real-time and historical view to network communications. • Logs can be used to perform analysis of authorized and unauthorized traffic flows. • Logs can be downloaded for offline analysis.
Person or Entity Authentication	164.312(d)	• Access is granted to authorized users after authentication. • Users can access applications only from designated/authorized workstations. • Person identity claim is validated with username to password mapping.
Transmission Security	164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii)	• Enforce encryption and integrity for data transmitted.

Physical Safeguards		
Workstation Use	164.310(b)	• Get visibility to and from which all workstations EPHI is being accessed. • Use tags to identify the workstations which can accessed the EPHI. • Enforce workstation + user based policies to control which all workstations can access EPHI. • Enforce application controls on workstation and servers to ensure that they are used only for specified purpose.



About ColorTokens

ColorTokens Inc. is a leading innovator in SaaS-based Zero Trust cybersecurity solutions, providing global enterprises with a unique set of products and services for securing applications, data, and users across cloud and hybrid environments. Through its award-winning Xtended ZeroTrust™ Platform and context-aware machine learning-powered technologies, ColorTokens helps businesses accurately assess and improve their security posture dynamically.

As cloud adoption grows, traditional perimeters get redefined, and new attack vectors and threat actors materialize, corporations recognize their security posture needs to reflect their Zero Trust philosophy. ColorTokens' technology allows customers to achieve Zero Trust by utilizing rich, meaningful contextual information about the application, microservice, or protected resource, so customers can apply Zero Trust with as secure of a perimeter as they can. ColorTokens' cloud-based SaaS platform can automatically deploy next-generation security controls and increase security posture dynamically without any new hardware, downtime, reboots, or changes to a client's existing systems.

For more information, please visit **colortokens.com**