COLORTOKENS

Technical Brief

MEETING HIPAA COMPLIANCE WITH THE COLORTOKENS XTENDED ZEROTRUST SECURITY PLATFORM

Introduction

ColorTokens helps healthcare organizations can meet HIPAA guidelines, limit the scope of their audits, and even accelerate the remediation of failed audits. The ColorTokens Xtended ZeroTrust Security Platform, based on a zero-trust architecture, can see, stop, and predict security and compliance violations across any workload, any deployment, and any user. Through a unified approach, healthcare organizations can simplify security and compliance throughout their modernization journey. ColorTokens is the only vendor that can, in a single 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 HIPAA regulated entities can overcome with ColorTokens.

HIPAA Specific Challenges

HIPAA compliance in healthcare can be exponentially 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:

- **Protect ePHI data:** Hospital staff and contractors constantly access 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 clueless about who is accessing what information, and why it is being accessed. ColorTokens provides comprehensive asset inventory of resources by storing, processing and transmitting ePHI. Security operators can see all incoming and outgoing traffic across critical assets and 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 and research data is driving up the number of cyber attacks in the healthcare industry. To protect the ePHI database, HIS applications, and other sensitive data, security teams need to understand the risks associated with these critical assets. ColorTokens provides a residual risk score and identifies high-value assets and their exposure levels. ColorTokens goes one step further, and provides security policy recommendations based on a proprietary risk metric. Users are also provided with a holistic risk score of their critical assets with the integration of the vulnerability management tool.

- **Ability to limit scope of an audit:** HIPAA audits can be costly. Failure of an audit is expensive in terms of escalating fines, reputational damage and loss of trust from patients and pharma partners. That being said, the cost of the audit can be an enormous expense itself, and the cost increases if the scope is not limited. The scope can be limited by showing auditable segmentation across the datacenter and multi-campus hospital locations.

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

Attack Vectors on Healthcare Environments

ColorTokens wants to ensure HIPAA regulated healthcare providers not only achieve compliance 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 areas:

- ***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 Attack:*** 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 Terminals Themselves:*** The lack of visibility of the inventory of assets and the configuration of a POS (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, and through visibility of assets across the organization.

HIPAA Mapping to the ColorTokens Xtended ZeroTrust Security Platform

A comparison of the HIPAA standards to the ColorTokens platform provides supporting evidence to an auditor, administrator, or an executive on how ColorTokens can ensure the safety and protection of customer and sensitive data. 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 Address by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
A	**Administrative Safeguards**		
1	***Security Management Process*** ***Risk Analysis:*** The potential security risks are identified, and the occurrence and magnitude are determined	164.308(a)(1)	Residual based risk metrics provides rich contextual insight into every business application & resources. Risk posture is quantified, and magnitude is determined based on OWASP principles. It continuously updates itself based on changes in the environment.

	HIPAA Requirement	Sub Requirements Address by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
	Risk Management: Sufficient security measures are available to reduce risks and vulnerabilities. Does the covered entity engage any third-party to assist in adopting risk management functions? ***Activity Review:*** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports		ColorTokens Xtended ZeroTrust Security Platform measures the risk of an asset and put it into application or resource group context by combining vulnerability information from third party tool, exposed attack surface and impact. ColorTokens Xtended ZeroTrust Security Platform provides flexible and adaptive policy engine mechanism which can be used to enforce policy on assets resulting is risk posture reduction and stopping the exploit of vulnerabilities. Provides visibility and audit of accesses, both made and blocked.
2	***Information Access Management*** ***Isolating health care clearinghouse functions:*** Restricting access to only those persons and entities with a need for access is a basic tenet of security. By implementing this standard, the risk of inappropriate disclosure, alteration, or destruction of E\ ePHI is minimized. Covered entities must determine those persons and/ or entities that need access to ePHI within their environment	164.308(a)(4)	Refer Access Control section.

	HIPAA Requirement	Sub Requirements Address by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
	Access establishment and modification: Covered entity must implement and manage the creation and modification of access privileges to workstations, transactions, programs or processes. Responsibility for this function may be assigned to a specific individual or individuals, which also may be responsible for terminating access privileges for workforce members		A user with Administrative privileges will be able to manage the CRUD operations.
3	***Security Awareness and Training***	164.308(a)(5)	
	Protection from malicious software: The workforce must also be trained regarding its role in protecting against malicious software, and system protection capabilities		The workforce must be regularly trained and should be aware of the critical role they play in protecting software and systems.
	Log-in monitoring: Information systems can be set to identify multiple unsuccessful attempts to log-in. Other systems might record the attempts in a log or audit trail.		In roadmap.

	HIPAA Requirement	Sub Requirements Address by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
4	***Contingency plan*** ***Emergency mode operation plan:*** When a covered entity is operating in emergency mode due to a technical failure or power outage, security processes to protect ePHI must be maintained	164.308(a)(7)	ColorTokens Xtended ZeroTrust Security Platform provides the ability to lockdown services, processes, daemons, and network activity to the bare minimum required for business needs.
B	**Technical Safeguards**		
1	***Access Control*** ***Unique user identification:*** Assign a unique name and/or a number for identifying and tracking user identity within information systems that contain ePHI ***Automatic logoff:*** System provides a feature to automatically logoff after a certain period of inactivity to prevent unauthorized users from accessing the ePHI ***Encryption and decryption:*** Mechanism is available to encrypt and decrypt electronic protected health information	164.312(a)(1)	A unique ID is assigned to the users based on the Active Directory (AD) properties. Session idle for more than 30 minutes, user needs to re-authenticate to re-activate the session. Enforces encryption on demand for services that do not natively secure communication or for administrator access to CDE. Every policy change is audit logged with user ID and timestamp.

	HIPAA Requirement	Sub Requirements Address by ColorTokens Xtended ZeroTrust Security Platform	How do We Address the Requirements
2	***Audit Controls***	164.312(b)	Every policy change is audit logged with user ID and timestamp.
3	***Person or entity authentication:*** Authentication mechanism is in place of the user to allow access to ePHI	164.312(d)	Every network access and session are recorded and made available through visual and textual means for deeper analysis. Nothing goes by unnoticed. ColorTokens Xtended ZeroTrust Security Platform policy engine ensures that only authorized accesses are allowed to protected entities.
4	***Transmission security*** ***Integrity Controls:*** Appropriate checks are in place ensure the ePHI transmitted using secure protocols ***Encryption:*** Ensure that the encryption mechanism adopted is as per the HIPAA Privacy rules	164.312€(1)	ColorTokens Xtended ZeroTrust Security Platform ensures integrity of data is maintained during communication between its protected entities. Uses TLS protocol during data transmission.

Conclusion

ColorTokens can ensure that healthcare organizations are prepared for HIPAA audits, can support ongoing compliance with HIPAA standards, and can help failed audits remediate faster. ColorTokens can limit the audit scope, provide cost savings and assure operational ease. Furthermore, with cloud compliance support, ColorTokens ensures that healthcare organizations are ready for their modernization journey, without the need for additional security or hardware investments, enabling the organization to focus efforts on providing better care to patients.

colortokens.com
sales@colortokens.com