AURORA Prime

HIPAA compliance Whitepaper

January 2024

Contents

OVERVIEW **5**
HIPAA Compliance Overview . . . 6

SECURITY GOVERNANCE **7**
HIPAA Administrative Safeguards . . . 7
Security Management Process . . . 7
Assigned Security Responsibility . . . 7
Workforce Security . . . 7
Information Access Management . . . 8
Security Awareness and Training . . . 8
Security Incident Procedures . . . 8
Contingency Plan . . . 9
Evaluation . . . 9
Business Associates Contracts and Other Arrangements . . . 9
HIPAA Physical Safeguards . . . 9
Facility Access Controls . . . 9
Workstation use & Workstation Security . . . 10
Device and Media Controls . . . 10
HIPAA Technical Safeguards . . . 10
Access Control . . . 10
Audit Controls and Integrity . . . 11
Person or Entity Authentication . . . 11
Transmission Security . . . 11
HIPAA Organizational Requirements . . . 11
Policies & Procedures and Documentation . . . 12

SECURITY SOLUTIONS **12**
Cloud Infrastructure . . . 12
Web Application Firewall - WAF . . . 12
Server Load Balancer - SLB . . . 13
SSL Certificates . . . 13
Container-based Architecture . . . 13
Auth Hub - Authentication & Authority . . . 13
Audit Trail - Audit Controls . . . 14
Monitor & Log Services . . . 14
Performance & Business Monitor Service . . . 14

Log Service 14

Appendix A – HIPAA SAFEGUARD AND SOLUTION MAPPING **15**

Notices **15**

Contents

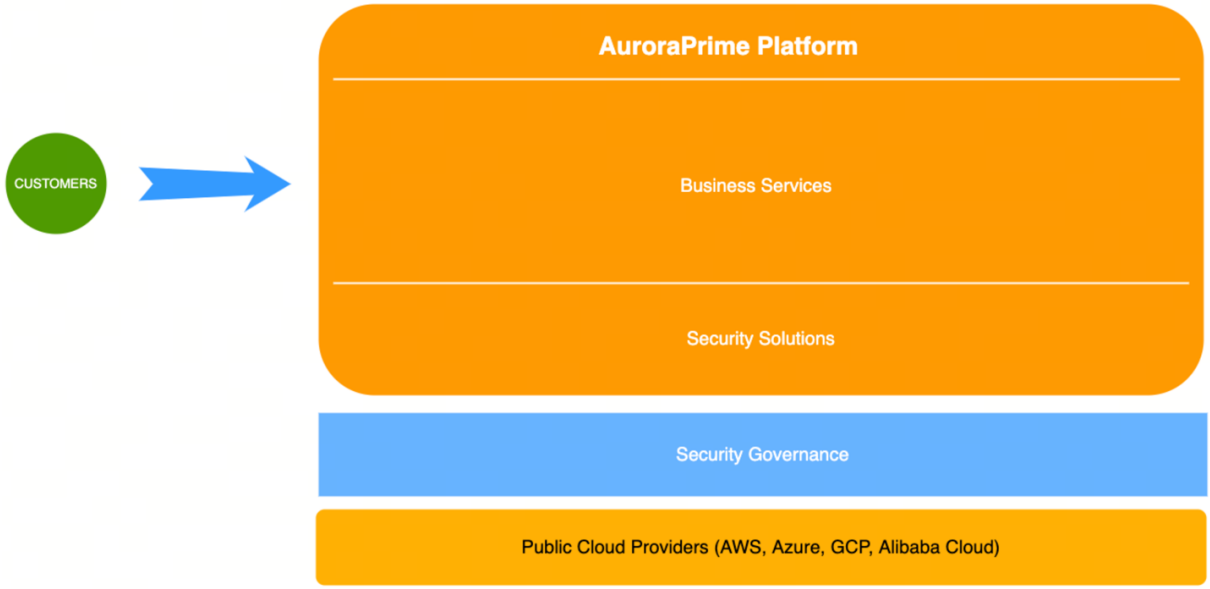
OVERVIEW

AuroraPrime, as a business platform of Shanghai Yaocheng Health Science & Technology Co., Ltd. (hereafter abbreviated as Yaocheng), provides a comprehensive suite of clinical trial services for its customers. This platform is offered to pharmaceutical companies to facilitate the storage of electronic Protected Health Information (ePHI). The architectural principle behind designing the platform is to establish a comprehensive software as a service (SaaS) platform, combining self-developed services, open-source middleware, and infrastructure from public cloud providers.

This paper describes AuroraPrime's HIPAA Compliance approach, with respect to the Security Rule, for implementing safeguards to protect the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). Protecting ePHI and compliance with the Security Rule is AuroraPrime's responsibility. This paper allows our customers to understand how the products and services offered by AuroraPrime address HIPAA security rules.

Achieving and maintaining HIPAA compliance includes administrative, physical, and technical safeguards. The elements for consideration of an integrated security approach include:

- AuroraPrime Security Governance: General information technology controls performed by AuroraPrime as part of normal business operations.
- AuroraPrime Security Solutions: Products and services that provide specific security implementations, which may provide primary protections to offer comprehensive solutions for some elements of the HIPAA security rule.



This paper is structured to provide detailed information regarding the security provisions of each of the following:

- AuroraPrime Security Governance
- AuroraPrime Security Solutions

HIPAA Compliance Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting 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 national standards for the protection of certain health information. The Privacy Rule refers to this information as "protected health information" (PHI). The Security Rule for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. 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). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance activities and civil money penalties.

HHS published a final Privacy Rule in December 2000, which was later modified in August 2002. This 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. Compliance with the Privacy Rule was required as of April 14, 2003 (April 14, 2004, for small health plans).

HHS published a final Security Rule in February 2003. This Rule sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information. Compliance with the Security Rule was required as of April 20, 2005 (April 20, 2006, for small health plans).

The Enforcement Rule provides standards for the enforcement of all the Administrative Simplification Rules.

HHS enacted a final Omnibus rule that implements a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information established under HIPAA, finalizing the Breach Notification Rule.

SECURITY GOVERNANCE

HIPAA Administrative Safeguards

An important step in securing electronic Protected Health Information (ePHI) is to implement reasonable and appropriate administrative safeguards that establish the foundation for a covered entity's security program, as addressed by §164.308 of the HIPAA Security Rule. In compliance with HIPAA administrative safeguards, AuroraPrime has implemented administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic Protected Health Information (ePHI) and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Security Management Process

AuroraPrime has defined a security management process to regulate overall strategies for information security and management procedures for the suite of products. This includes defining the responsibilities of members and business units within AuroraPrime's information security. AuroraPrime has established policies to regulate information security risk identification and assessment procedures, etc. AuroraPrime has established policies and procedures for governance and risk management, information security management, IT operations, etc. To effectively govern the people elements of the business, AuroraPrime also provides learning and awareness training for all employees, including company culture, vision, security, and privacy. Professional training on data protection offered by internal and external experts is also available to employees.

Assigned Security Responsibility

The AuroraPrime Information Security Strategy directs the strategies for information security and management procedures for the information security program. Based on this strategy, AuroraPrime has established guidelines to define the responsibilities and roles of members within the organization's information security structure. These responsibilities include monitoring information security incidents, coordinating security awareness training exercises, and providing resources to support internal audits and risk assessments.

Workforce Security

AuroraPrime has policies and procedures in place addressing workforce access to ePHI concerning the clearance of employees, appropriate employee authorizations, and termination processes. Background checks on prospective employees, depending on role and position, are documented in the

human resources management system. Employees are required to sign a confidentiality agreement and acknowledge the employee code of conduct. Vendors are required to sign a contract and confidentiality agreement as well as a business associate agreement, if deemed to be a covered entity.

Information Access Management

AuroraPrime has policies and procedures in place surrounding logical access management, including basic rules for the segregation of duties per user role or responsibility, and appropriate controls over the enterprise user access management system. All access requests (provisioning and modification) submitted by users for normal and privileged accounts are logged within the aforementioned access management system and are only authorized after proper review and approval by management, based on risk level and minimum access necessary. Separated employees are removed via an automated process triggered by the individuals being disabled within the human resources management system. This is to ensure that only specific users have access to ePHI and related systems as well as configuration settings.

Security Awareness and Training

Yaocheng sets up a security team responsible for developing a Security Awareness Training (SAT) program. This program is provided for employees to promote information security awareness and ensure policies regarding business conduct are known within the organization. All relevant policies and procedures are currently available on internal platforms and are easily accessible for employees.

To mitigate the possibility that malicious software compromises information systems housing ePHI, Yaocheng only authorizes specific channels to download software onto PCs and pushes antivirus software to physical servers and workstations as a means of protection from malware attacks and other potential cybersecurity threats.

Security Incident Procedures

AuroraPrime has a robust security incident response plan in place to identify, address, and remediate information security incidents (the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system with access to covered information). In the event of an incident, AuroraPrime has an expansive network of communications including text messages, emails, and online bulletin board posts to relay the appropriate information to the specified responsible parties. The procedures in place address classification of security incidents, establish definitions for timely response, and detail corresponding solutions to security incidents according to incident level.

Contingency Plan

As a means of assuring that AuroraPrime is prepared for any sort of event that could result in data being compromised, a variety of plans have been developed to demonstrate readiness. AuroraPrime currently performs a business continuity drill at least once a year with business continuity reports being issued accordingly. In addition to this, AuroraPrime has established targeted emergency response plans for identified technical failures of products and provided services, which are designed to reduce the impact on the potential end user in the event of an emergency or incident.

Evaluation

AuroraPrime has several policies and procedures in place to govern change management processes and ensure that all environmental and operational changes that would affect the security of ePHI are reviewed by information security management and other executive management on a periodic and ad-hoc basis.

Business Associates Contracts and Other Arrangements

AuroraPrime requires vendors to sign contracts and confidentiality agreements; rights and obligations, scope of services, compliance requirements, and service levels are detailed within vendor service contracts. The customer and vendor contracting process is centralized, and all customers and vendors are assessed to determine whether they are covered entities and therefore whether they require a business associate agreement.

HIPAA Physical Safeguards

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate physical safeguards for information systems and related equipment and facilities, as addressed by §164.310 of the HIPAA Security Rule. In compliance with HIPAA physical safeguards, AuroraPrime has implemented physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Facility Access Controls

Yaocheng has policies and procedures in place that specify the processes to access the room which stores archives. Employees who need to access archives need to sign an acknowledgment of archives

access table and also need permission from the executive management team. In addition, Yaocheng has established an IT room which is managed by specialized people. Other than those people who want to enter the IT room, they need to be approved by executive team members.

Workstation use & Workstation Security

AuroraPrime has policies and procedures in place that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of enterprise workstations that can access ePHI or sensitive customer data. Employees are required to sign an acknowledgment of AuroraPrime's acceptable server use and the enterprise code of conduct. Servers that have access to, transmit, store, or otherwise process ePHI are physically protected from unauthorized use, including, in particular, those housed in public cloud providers.

Device and Media Controls

AuroraPrime has policies and procedures in place regarding the management of devices and media that access, store, or transmit ePHI. These policies stipulate that storage media to be discarded must be physically destroyed on the premises, thereby mitigating the risk of the media being accessed by unauthorized individuals or entities. The destruction and disposal of hardware and media containing sensitive information are recorded and maintained. IT asset identification and classification are included as part of the annual information security risk assessment process and are kept up-to-date on an ongoing basis.

HIPAA Technical Safeguards

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate technical safeguards for information systems that represent best business practices for technology use and configuration, as well as associated technical policies and procedures. In compliance with HIPAA technical safeguards, AuroraPrime has implemented several security measures and technical solutions that allow it to reasonably and appropriately implement the standards and implementation specifications.

Access Control

AuroraPrime has policies and procedures in place governing logical access controls, including basic rules for the segregation of duties by varying roles and functions based on the company structure and product teams, as well as processes surrounding the centralized access management system. All

access requests for normal and administrator accounts within the system require authorization and reviews by management to determine if access to the requested accounts is feasible based on the associated risk level. In addition, AuroraPrime has established General Access Control strategies that require the segregation of production and non-production environments into different network security domains.

Audit Controls and Integrity

AuroraPrime has a log management platform in place to monitor and record user operations at a network level, and for the AuroraPrime product suite; log retention is configured within the system. Additionally, integrity checks are performed by AuroraPrime to compare currently stored data and information to previous states as a means of ensuring that changes have not occurred and, if they have, that they could not cause the data to be altered or manipulated in a malicious way.

Person or Entity Authentication

AuroraPrime has policies and procedures in place to ensure that user and entity accounts undergo proper authentication measures. Customer attempts to access AuroraPrime product suites require authentication by the use of the provisioned global unique ID ("UID") to validate their legitimacy. When authentication fails, the user will be sent back to the login console and will not be granted access to the product. In addition to this, AuroraPrime supports two-factor authentication based on the password and a one-time password (OTP) to authenticate users.

Transmission Security

AuroraPrime has established transmission security management policies and procedures that specify security management requirements and measures taken to ensure that data is transmitted securely. The data encryption services (provided by public cloud providers) used by AuroraPrime meet the requirements of the State Cryptography Administration and are certified thereby. Therefore, AuroraPrime supports secure communication channels with cryptographic protocols such as HTTPS. For applicable products, data-at-rest encryption is also considered, leveraging solutions provided by public cloud providers.

HIPAA Organizational Requirements

An important step in protecting electronic Protected Health Information (ePHI) is to implement reasonable and appropriate organizational safeguards for important information security governance

and HIPAA-mapped policies and procedures.

Policies & Procedures and Documentation

AuroraPrime, in compliance with ISMS/ISO 27001 requirements, has policies and procedures in place that ensure the organization's development and documentation of formal policies and procedures, requiring their existence, and periodic review and maintenance. AuroraPrime's policies and procedures detail retention periods for policy documentation, which comply with HIPAA (6-year minimum). Policies and procedures are reviewed and updated annually, as required by ISO 27001 and in compliance with HIPAA. The documented policies and procedures are made available to individuals responsible for implementing the procedures to which the documentation pertains via AuroraPrime's internal platforms.

SECURITY SOLUTIONS

AuroraPrime is fortified with a wealth of technical security measures addressing HIPAA technical safeguard requirements. AuroraPrime achieves this by building high-availability applications; providing account authentication and authorization services that support two-level account credentialing for ease of segregation of duties, multi-factor authentication, group authorization policies, fine-grained access control, and tokenization; providing security audit support, and data encryption support.

The following solutions are part of the security architecture offered within AuroraPrime solutions and include an overview of the product, a description of the key security features available, and a reference to the related HIPAA security rule specification.

Cloud Infrastructure

Web Application Firewall - WAF

Web Application Firewall (WAF) is a SaaS-based web application security service that detects illegal web requests through its built-in security strategy, thereby protecting your website servers against intrusions. AuroraPrime leverages WAF, provided by cloud providers, to detect and block malicious traffic directed at our websites and applications. WAF secures our core business data and prevents server malfunctions caused by malicious activities and attacks.

Server Load Balancer - SLB

SLB is a server load balancing service used to distribute incoming traffic among several cloud servers. SLB extends the external service capability of application systems by traffic distribution. It improves the availability of application systems by eliminating a single point of failure.

SSL Certificates

Leveraged by the SSL Certificates Service of public cloud providers, AuroraPrime is hardened as HTTPS-secured websites to encrypt the communications between users and the websites, ensuring that traffic is adequately protected from hijacking, snooping, and tampering [§164.312 (e)(2)(ii) Transmission Security – Encryption].

Container-based Architecture

AuroraPrime is based on a microservice architecture. Its applications run within containers. The platform is based on solid infrastructure provided by public cloud providers. Leveraged by Virtual Private Cloud (VPC), AuroraPrime's production environment is isolated from other environments. AuroraPrime has policies and procedures in place to allow employees to access AuroraPrime's production environment.

Leveraged by Kubernetes Management Service (KMS), products of AuroraPrime are running within a scalable Kubernetes cluster which confirms the high availability of the AuroraPrime platform. ## Core Services

Auth Hub - Authentication & Authority

Auth Hub, the core service of the AuroraPrime platform, is responsible for authentication and authority management. Functionally, the service has the following solid functions, considering a variety of security aspects:

- Implements SAML 2, OAuth 2, OpenID Connect, and other protocols as SP, which can easily be integrated with internal and external identity authentication systems.
- Implements basic user group management functions and allows group-based permissions control, such as who can access which applications.
- Implements basic organizational concepts and allows users to join multiple organizations. Organization administrators can manage users' organizational relationships, allowing autonomy within the organization and reducing the need for super administrators to intervene.

Audit Trail - Audit Controls

Audit Trail, the core service of the AuroraPrime platform, is responsible for recording user operations. An Audit Trail service records user operations in the following formats to keep data integrity:

- User
- Timestamp
- Operation object
- Operation type
- Operation content
- Labels
- Source

Monitor & Log Services

Performance & Business Monitor Service

The Monitor service collects monitoring metrics of AuroraPrime resources (CPU, MEM, DISK) as well as product-defined metrics. The Monitor service enables the AuroraPrime OPS team to view and fully understand the usage of AuroraPrime resources, and the status and health of the platform business, so that the AuroraPrime OPS team can act promptly to ensure the availability of your application when an alarm is triggered.

Alarms are configured to trigger based on preset rules set by the OPS team based on usage, performance, and operational state [§164.312 (b) Audit Controls] [§164.308 (a)(1)(ii)(D) Information System Activity Review].

Log Service

AuroraPrime has set up a self-hosted log service. This is a complete real-time data logging service. Log Service supports the collection, consumption, shipping, search, and analysis of logs, and improves the capacity of processing and analyzing large amounts of logs.

The prominent security features of this service are that log data collected by the product is stored with high reliability and tampering prevention, so that on an append-only basis users can add to logs but cannot modify or alter previous logs, maintaining log integrity [§164.312 (c)(1) Integrity]. Additionally, the log service complies with HIPAA security rules such as [§164.308 (a)(7)(ii)(A) Contingency Plan – Data Backup Plan], [§164.312 (a)(1) Access Control].

Appendix A – HIPAA SAFEGUARD AND SOLUTION MAPPING

		HIPAA Security Rule Safeguards Addressed								
		§164.308(a)(1)(ii)(D) Information System Activity Review	§164.308(a)(5)(ii)(B) Protection from Malicious Software	§164.308(a)(5)(ii)(c) Log-in monitoring	§164.308(a)(5)(ii)(D) Password Management	§164.308(a)(7)(ii)(A) Data Backup Plan	§164.312(a)(1) Access Control	§164.312(a)(2)(iv)Encryption and Decryption	§164.312(b) Audit Controls	§164.312(c)(2)(i) Transmission Security - Integrity Controls
Security Solutions	WAF		☑				☑			
	SLB						☑			
	Container based Architecture	☑					☑			☑
	SSL							☑		☑
	Auth Service		☑		☑					
	Audit Service	☑								
	Monitor Service	☑	☑			☑			☑	☑
	Log Service	☑		☑		☑			☑	☑

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only; (b) represents current AuroraPrime product offerings and practices, which are subject to change without notice; and (c) does not create any commitments or assurances from Yaocheng. AuroraPrime products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Yaocheng to its customers are governed by user agreements, and this document is not part of, nor does it modify, any agreement between Yaocheng and its customers.