
HIPAA Platform Security & Compliance

Overview for Cardiac Centers (Version 2026.3)

CONTACT INFORMATION:

Adam Pick, Founder

(310) 990-3401

adam@heartvalvesurgery.com

Table of Contents

Executive Summary	3
About the HeartValveSurgery.com Platform	3
Platform Architecture	4
Service Providers	5
Security Features	5
Online Analytics Tracking Technologies	7
HVS Web Application Infrastructure Provider Audit Compliance	8
Virtual Chief Information Security Officer	9
For Additional Information	9

01

Executive Summary

Heart Valve Interactive Corp., the owner and operator of HeartValveSurgery.com (“HVS”), is serious about protecting and securing the information technology systems that power its patient recruitment platform (the “Platform”). We are committed to implementing procedures and policies designed to secure and to protect the data and the processes within the Platform.

For this reason, HVS has developed an interactive environment with security documentation that has been reviewed by a qualified, external third-party with a completion date of March 23, 2026, including confirmation that HVS is in compliance with HIPAA Security Rule §164.308, §164.310, §164.312, §164.314 and §164.316. This document describes the security strategies and safeguards within the Platform.

02

About the HeartValveSurgery.com Platform

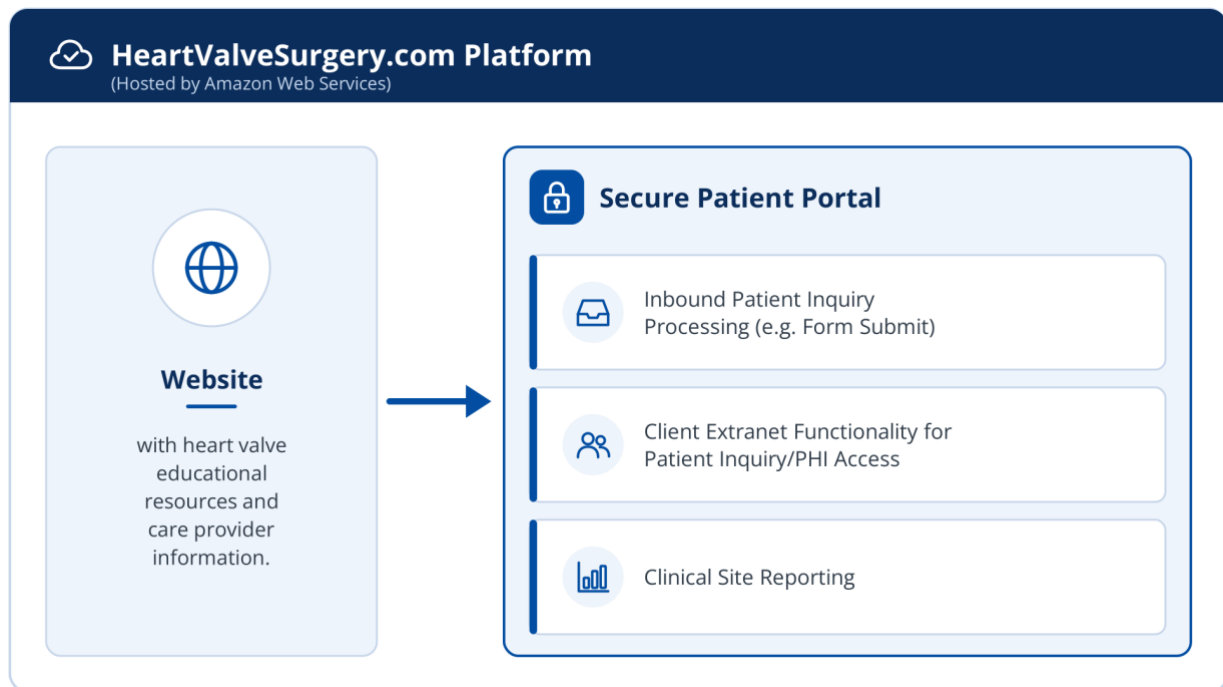
HVS generates new patient acquisition for cardiac centers using novel technologies across the HVS platform. HVS drives patient awareness to care providers and then enables patients to “self-refer” to those cardiac centers dedicated to heart valve therapy (the “Patient Recruitment Process”).

Our sponsors, which include hospitals and health systems (e.g. the Cleveland Clinic, Cedars-Sinai Medical Center and Northwestern Medicine) use the HVS cloud-based patient portal (the “Patient Portal”) which provides immediate and ongoing access to protected health information (“PHI”) to support the Patient Recruitment Process.

Platform Architecture

The Platform leverages integrated systems that enable patients to learn about therapies, to research potential care providers and to connect with cardiac centers.

The Patient Recruitment Process occurs within an environment designed to be secure that deploys various technologies, resources and assets described in the schematic shown on the next page.



A brief description of the Platform architecture is provided below.

1

Website: The HVS web application is hosted on HIPAA-eligible AWS infrastructure under a Business Associate Agreement (BAA); HVS remains responsible for its HIPAA compliance obligations.

2

Patient Portal: The HVS Patient Portal is hosted on HIPAA-eligible AWS infrastructure under a Business Associate Agreement (BAA); HVS remains responsible for its HIPAA compliance obligations.

3

Extranet: Clients gain access and visibility to patient records and PHI within the Patient Portal using secure access points that require a complex password and multi-factor authentication.

04

Service Providers

To develop, implement and manage the Platform, HVS integrates best-of-breed service providers across the Platform.

It is important to note that:

- Each service provider specializes in information technology solutions that are designed to be both secure and HIPAA compliant.
- HVS ensures that business associate agreements (BAA) are in place with all service providers that store or handle protected health information across the Platform.

05

Security Features

HVS utilizes a technology environment including, but not limited to, the following HIPAA compliant safeguards that are implemented through a robust defense-in-depth strategy:



01

AWS CloudFront Gateway and AWS Security Groups

An AWS CloudFront Gateway is utilized to monitor and log all incoming and outgoing network traffic to the HVS AWS Virtual Private Cloud via VPC flow logs, and AWS Security Groups allow minimum necessary ports and services to reduce our internet attack surface and limit external exposure of our information technology environment.



02

Web Application Firewall & Dynamic Application Security Testing

A web application firewall is utilized to protect our websites from common OWASP attack methods, such as SQL Injection, Cross Site Scripting, Sensitive Data Exposure, and other potential vulnerabilities. In addition, a qualified third party completed dynamic application security testing of the HVS web application in 2026, with confirmation that HVS remediated all identified, recommended high and medium vulnerabilities



03

Multi-factor Authentication for Administrative and User Access

Administrative staff with elevated privileges and users with non-elevated privileges to our technology environment are required to use multi-factor authentication in order to log on and complete administrative and non-privileged duties.



04

Anti-virus Protection

Industry class anti-virus protection is utilized throughout our technology infrastructure and is designed to prevent malicious and unauthorized malware, viruses, and code from executing.



05

Server Hardening and System Logging and Monitoring

All servers in our technology infrastructure are subject to a security review, with unnecessary services disabled, security and configuration settings reviewed and tuned, logging enabled, and default passwords changed. System logs are monitored on a routine basis to identify and pinpoint errors or evidence of malicious activity.



06

Data Backup and Recovery

A robust data backup and recovery strategy is in place and designed to ensure that our system and data is backed up and can be restored if needed.



07

Business Continuity and Disaster Recovery planning and capability

Our technology environment is operated with an enterprise business continuity and disaster recovery plan designed to ensure that the system and all data are highly available.



08

Secure, encrypted connectivity and database

The websites we leverage utilize TLS-encrypted connectivity, which is designed to ensure that all user credentials and sensitive data in transit are protected with encryption standards that are in compliance with Federal Information Processing Standard (FIPS) 140-3 (where validated cryptographic modules are used; verification required). The HVS web application database is encrypted at rest.

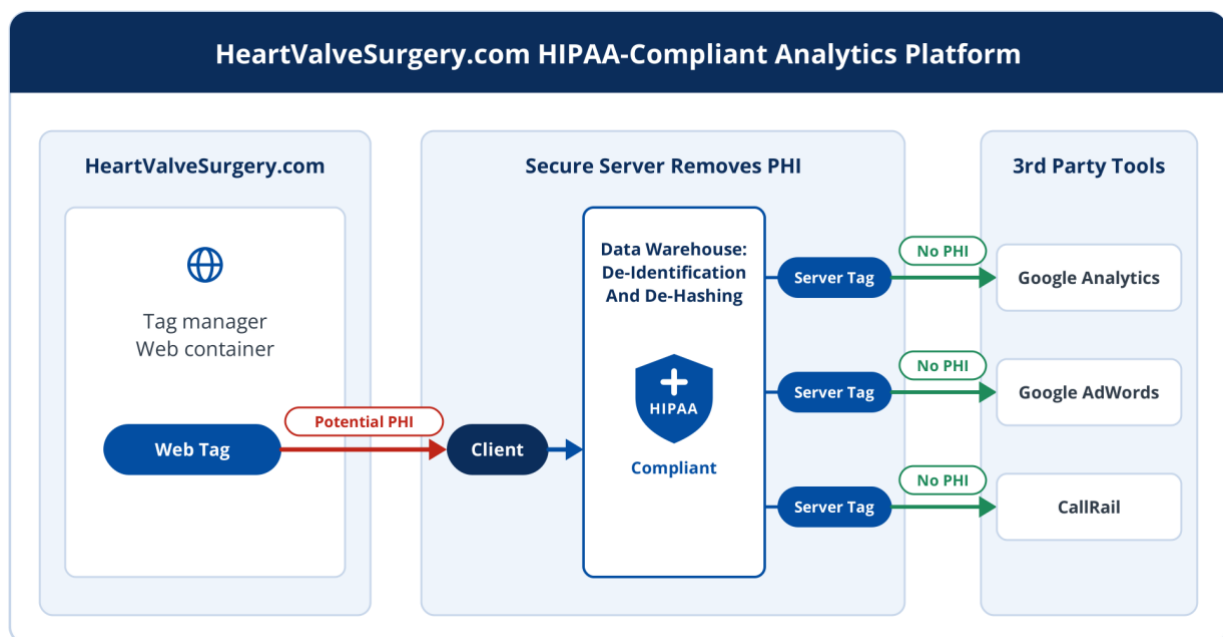
Online Analytics Tracking Technologies

In December 2022, the Department of Health & Human Services (HHS), which oversees HIPAA regulations, released new guidance shedding light on how to avoid sharing individually identifiable personal health information with tracking platforms or technologies like Google Analytics, the Meta Pixel and more (the “HHS Bulletin”).

HHS revised its tracking-technologies bulletin in March 2024; in June 2024, a federal court in *ABA v. Becerra* vacated the guidance insofar as it treated certain unauthenticated public webpage visits as disclosures of individually identifiable health information based solely on IP address and visits to health-related webpages.

Upon review of the HHS Bulletin, the HVS security, compliance and legal teams began evaluating various strategies and approaches to adhere to the HHS Bulletin while continuing to effectively use key performance analytics in a HIPAA-compliant environment. That analysis included (i) an exhaustive review and test of third-party service provider applications and (ii) the development of internal solutions.

After completing the analysis, HVS elected to deploy an internally developed solution with select technology partners, under Business Associate Agreements, that appropriately collects and reports key performance analytics for the HVS platform in a HIPAA-compliant environment.



As shown the schematic on the prior page, the solution leverages an agnostic analytics engine, a data warehouse, de-identifying transformations within the data warehouse, and other strategies to report key performance indicators in a HIPAA-compliant environment.

As a result, HVS can adhere to the guidance provided within the HHS Bulletin and continue to leverage analytics for the effective management of this patient-centric platform.

07

HVS Web Application Infrastructure Provider Audit Compliance

The Platform leverages services that have comprehensive privacy and security assessments and certifications performed by third-parties including:

✓ ISO 27001/27018

✓ SSAE 16/ISAE 3402 SOC-1

✓ SOC 2 and SOC 3

✓ PCI-DSS

✓ TRUSTe Certified Privacy Seal

✓ CSA Star

✓ EU / EEA and Switzerland Safe Harbor

✓ FedRAMP

✓ TUV Rheinland Certified Cloud Service



08

Virtual Chief Information Security Officer



Andrew Labbo, MBA, CISSP, is the Virtual Chief Information Security Officer of HVS. Andrew has over 25 years of experience with information security and technology and over 10 years of experience as a privacy and data security officer. Andrew is an expert on HIPAA Privacy and Security Rule regulations as well as HITECH and Omnibus regulatory updates.

09

For Additional Information

To learn more about the security features of the HVS Platform, please contact Adam Pick, the founder of HVS, at (310) 990-3401 or adam@heartvalvesurgery.com.

© 2026 Heart Valve Interactive Corp. All Rights Reserved.

Revision review: October 22, 2026. Version 2026.3 retained; technical configuration and certification claims remain subject to verification.