Introduction

Precision.heart.org offers a state-of-the-art data marketplace that includes data, tools and a secure, cloud-based workspace for performing scientific research.

Security Summary

Precision.heart.org provides an in-depth security architecture. The platform currently supports research data without Protected Health Information (PHI).[1,2] To provide assurance the platform will protect data appropriately, Precision.heart.org will receive the following attestations:

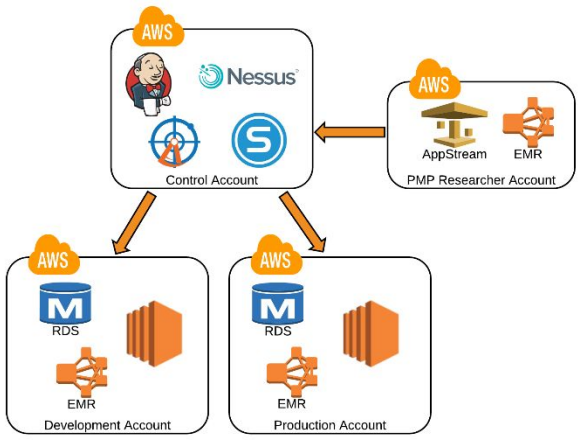
Standard	Description	Date
HIPAA	HIPAA Compliant Environment validated by 3rd party	July 2017
FedRAMP	Low certification granted	June 2018

Platform Security Controls

Precision.heart.org uses a combination of security measures. Below is a brief description of some of the most critical:

Administrative Environment Access and Separation of Duties

Precision.heart.org utilizes the concept of "Control Accounts" for the application environments. A Control Account is used as a common area for hosting shared services and administrative tools that run against the "Managed Accounts". This allows the platform to reduce and simplify the amount of administrative privileges required to manage production services while maintaining high levels of manageability.



In this diagram, the Control Account is used to manage:

Jenkins and all pipeline deployments into the Dev and Prod accounts

Nessus vulnerability scans into the other accounts

REAN Radar

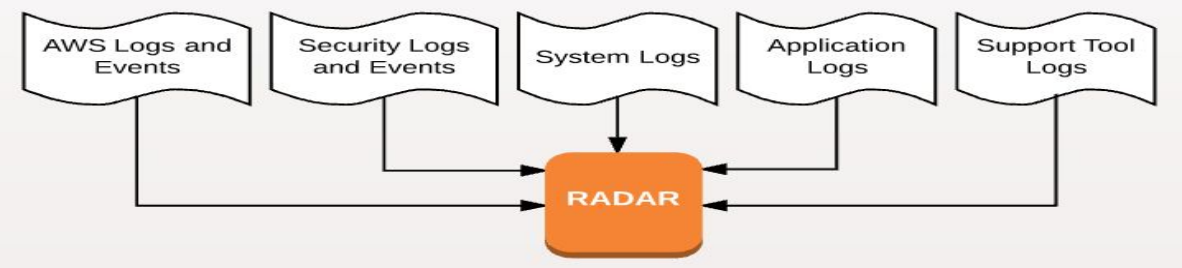
Pipelines for administrative access into the other environments eliminate the need for direct access into sensitive areas of the platform

[1] https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

[2] The PMP may include PHI in the future if the research community requires and will then perform the necessary actions to achieve FedRAMP Moderate status.

Logging, Monitoring and Continuous Compliance

Tracking how an environment changes over time, and who accesses it, is central to meeting many different regulatory and data access control requirements. To paint the full picture of what is occurring in the AHA-PMP, we store application logs, operating system logs, AWS service logs and other environment specific logs and performance data. This all must be organized and retained for potential use during troubleshooting activities or compliance audits.



Radar ingests logs from many different sources, configures meaningful dashboards of information relevant to the environment, and evaluates that information in the context of well-respected security and compliance frameworks such as Center for Internet Security (CIS) benchmarks. Radar dashboards monitor for configuration drift, changes to sensitive data access, misconfigured infrastructure, broken ingest pipes, and numerous other AHA-PMP specific metrics and measures. Specific dashboard monitors in real time who has access to controlled datasets.

Encryption

All data stored within the platform receives encryption whether in motion, going through processing or at rest. The platform utilizes “envelope encryption” which provides multiple layers of 256-bit encryption in a manageable system, and is integrated into the monitoring system, RADAR, that provide you with key usage logs to help meet our auditing, regulatory and compliance needs.

Data Security

The security ecosystem on Precision.heart.org is established to protect the access controls around consents and committees within sponsoring organizations. Levels of access range from simple, “one click” access to more involved “three click” access steps. As access is granted, pipelines within the platform immediately enable read only access to the requester.

User Roles

The platform currently supports three types of primary users:

User Type	Learn	Search (Portal)	Individual Workspace	Other Workspaces (Based on Permissions)	Community
Registered User	X	X			X
Approved Researcher	X	X	X		X
Shared Workspace Researcher				X	