Artemis Security Brief

Security is one of our core values.
We go above and beyond to protect your data.

Learn more about the
Artemis Platform at:

artemishealth.com

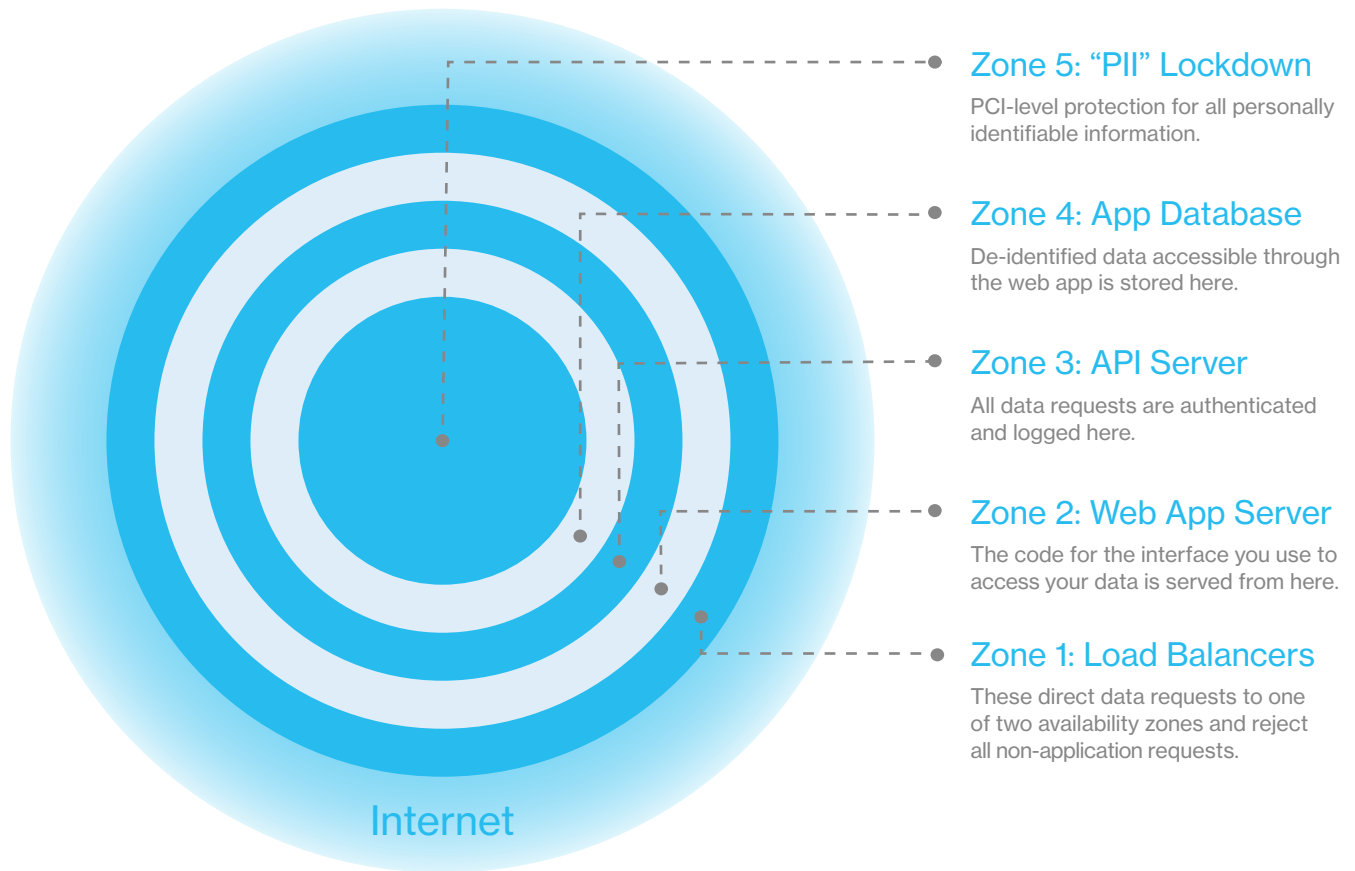## Table of Contents

01 Artemis Security Architecture

Our industry-leading hardened cloud architecture keeps increasingly sensitive data in increasingly secure zones.

Lockdown

Each zone can only communicate with the zone protecting it. This means an intruder would need to break through all five firewalls, each requiring unique access keys, before they could reach any sensitive daya. There is a wall around all zones keeping them private from the internet.

Full redundancy

We maintain two identical environments in two separate data centers to make sure your data is always available.

Zone 5: "PII" Lockdown

PCI-level protection for all personally identifiable information.

Zone 4: App Database

De-identified data accessible through the web app is stored here.

Zone 3: API Server

All data requests are authenticated and logged here.

Zone 2: Web App Server

The code for the interface you use to access your data is served from here.

Zone 1: Load Balancers

These direct data requests to one of two availability zones and reject all non-application requests.

Internet

02 Fully HIPAA Compliant

We go above and beyond all HIPAA recommendations
to ensure the highest level of security.

Technical HIPAA recommendations
All data is encrypyted while stored and while being transferred or accessed. All
data access has a full audit trail and is governed by role-based access controls.

Data de-identification
Before we make your data available for analysis, we de-identify it according to
the guidelines published by Health and Human Services.

HIPPA policies & procedures
All policies are defined in coordination with HIPAA-specialized legal counsel
(the same counsel that defined Intermountain Healthcare's HIPAA policies).

- Policies are reviewed *quarterly* for adherance assurance.
- Polices are reviewed *annually* for changing requirements.

Selected Artemis HIPAA Policies

- Business continuity
- Incident response
- Patch management
- Incidence remediation
- Employee pre-screening
- Employee provisioning
- Employee termination
- Employee role-change
- Unlocking / resetting employee accounts
- Onboarding new customers
- Adding new customer users
- Unlocking / resetting a customer account

For more detailed information about HIPAA compliance, review
the guidelines on Health and Human Services's website:
http://www.hhs.gov/ocr/privacy/

03 End-to-End Encryption

When data is transfered into, out of, or stored inside the Artemis platform, it's always encrypted.

"At rest" encryption
Data not currently in use is encrypted at the highest feasible level (256-bit AES). This includes backups.

"In flight" encryption
The platform rejects all unencrypted connections. No exceptions.

Only designated Artemis operations team members can access the platform outside the normal user interface. In order to do maintenance, they must use direct network or VPN (virtual private network) access that requires 2-factor authentication.

Database and system access is secured with 2048-bit encryption.

Web access also requires 256-bit encryption (i.e. SSL, which is what Amazon uses to secure online purchases).

04 Strict Authentication & Audit

Strict authentication and auditing means you're always in control of who sees what data and when they see it.

Authentication security

- Strict password complexity and change frequency requirements.
- Account lockout after 4 failed login attempts.
- Requires customer support to unlock.

Audit trails

- Full audit trail by user of every piece of data accessed.
- No shared accounts allowed to ensure the integrity of the audit logs.

What is encryption?

The translation of data into a secret code. Encryption is the most effective way to achieve data security.

To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Unencrypted data is called plain text. Encrypted data is referred to as cipher text.

The difficulty of breaking encryption is measured in "bits" (e.g. 256-bit encryption is very strong).

To learn more, start here: https://www.webopedia.com/definitions/encryption/

05 Internal Controls & Training

We foster a culture of security within Artemis to ensure compliance at all times.

Technology development

1. Infrastructure, codebase, and database access individually restricted to operations teams personnel only.
2. Infrastructure access requires two-factor authentication in addition to standard credentials.
3. Developers are trained on application security best practices.

Account security

1. All accounts have role-based access restrictions.
2. New accounts are only created with proper documentation and authorization.
3. Changes to account access are only permitted with proper documentation and authorization.

06 Threat Management

Both our platform and our office infrastructure are locked down and tested regularly.

Office security
All Artemis computers and devices have encrypted hard and auto-updated anti-virus software installed. Intrusion detection monitoring both in offices and in the data center.

Platform security

- Monthly automated penetration testing.
- Human-performed penetration tests at least yearly.
- Application vulnerability scans run monthly and after every deploy of new server-side code.

What is penetration testing?

A penetration test, or "pen test," is an attack on one's own computer system by one or an authorized party with the intention of finding security weaknesses, potentially gaining access to it, its functionality, and its data. Both technological vulnerabilities and human vulnerabilites are exploited by "hacking" and "social engineering," respectively.

To learn more, start here: https://en.wikipedia.org/wiki/ Penetration_test

07 Data Center Certificates & Security Features

Our platform is hosted in the AWS cloud because no other data centers on earth have more security certifications or policies and controls.

Cloud-based = more secure
95% of all health data breaches in 2012 resulted from physical media loss or theft (e.g. the computer hosting the data, a thumb drive, paper, etc.) according to HITRUST*. In a cloud environment such as AWS, tracking down the physical server on which data is hosted is virtually impossible, thus mitigating the risk of loss.

Security inherited from AWS
AWS has built-in protections against:

- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle (MITM) Attacks
- IP Spoofing
- Much, micu more

Learn more about AWS
You can read about AWS' security features here:
http://aws.amazon.com/security/

You can read about AWS' compliance measures here:
http://aws.amazon.com/compliance/

Selected AWS Certifications

- SOC1 / SSAE 16 / ISAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- PCI DSS Level 1
- ISO 27001
- ITAR
- FIPS 140-2
- HIPAA
- Cloud Security Alliance (CSA)

08 Processing Integrity

Artemis maintains data pipeline integrity with several automated validations through each stage of the data pipeline.

Artemis maintains data pipeline integrity with several automated validations through each stage of the data pipeline. Additionally, we ensure high data quality via hundreds of data checks for accuracy, completeness, and consistency. Our team of healthcare Data Management experts is equipped with the tools to inspect and resolve any potential quality concerns detected through these processes.

Make better data-driven decisions with Artemis Health.
Get in touch to learn more.

artemishealth.com/measure

hello@artemishealth.com