SECURITY & PRIVACY WHITE PAPER

ResiCareHealth OS

Security architecture, HIPAA-oriented governance, data protection, and operational safeguards

Purpose of this document

This paper summarizes the safeguards and governance practices ResiCareHealth uses to protect sensitive healthcare information and support customer security and compliance due diligence.

Version 1.0 | August 14, 2026 | www.resicarehealth.com

01 Executive Summary

Security designed around the confidentiality, integrity, and availability of resident and customer information.

ResiCareHealth OS is a cloud-based operating platform for residential assisted living organizations. Because the platform may create, receive, maintain, or transmit protected health information (PHI) and electronic protected health information (ePHI), ResiCareHealth treats information security and privacy as core operating requirements, not optional product features.

The ResiCareHealth security program is structured around the administrative, physical, and technical safeguard concepts in the HIPAA Security Rule. HHS describes the Security Rule as requiring appropriate safeguards to protect the confidentiality, integrity, and availability of ePHI.[1] ResiCareHealth has developed supporting policies, risk-management procedures, incident-response processes, workforce security requirements, vendor review practices, backup/recovery procedures, and an evidence-management framework to operationalize those expectations.

Important compliance statement

ResiCareHealth does not represent this white paper as a government certification, legal opinion, or independent audit. HHS does not certify products as "HIPAA compliant," and HIPAA compliance depends on actual practices, documented safeguards, contractual obligations, risk management, and the way each customer uses the system.[2]

Security posture snapshot

Security Area	Status	Prospect-Facing Summary
Security Risk Assessment	**Completed**	Completed SRA feeds the formal risk-management process.
Security / privacy governance	**Established**	Policies cover risk, training, incidents, recovery, access, vendors, review, and evidence.
AWS privileged access	**Implemented**	Administrative access uses MFA and least-privilege principles.
Amazon S3 encryption	**Implemented**	S3 provides default server-side encryption for new objects.[6]
AWS CloudTrail	**Implemented**	CloudTrail supports AWS activity logging and audit visibility.[7]
AWS-native backup	**Implemented**	AWS-native backup capabilities support data protection and recovery.
PostgreSQL & control evidence	**Implemented**	Database encryption controls are in use; supporting configuration evidence is maintained through the compliance evidence process.

02 Security Governance & Risk Management

Documented responsibilities, repeatable risk decisions, and evidence-based remediation.

Risk-based security management

ResiCareHealth maintains a Security Risk Management Plan designed to identify threats and vulnerabilities, evaluate likelihood and impact, document existing safeguards, assign remediation owners, track target dates, collect implementation evidence, and reassess residual risk. This aligns with HHS guidance that risk analysis is the first step in identifying and managing risks to ePHI.[3]

- Identify the system, application, vendor, process, threat, vulnerability, or control gap.
- Document existing safeguards and the evidence available to support them.
- Rate likelihood and potential impact using a consistent internal scoring method.
- Assign corrective action, accountable ownership, and a target completion date.
- Collect evidence that corrective action is operating as intended.
- Reassess residual risk and formally close, monitor, transfer, or accept the risk.

Governance documentation

Security Risk Management Risk identification, prioritization, remediation tracking, and residual-risk decisions.	**Security Training** Workforce security awareness, role-appropriate education, and signed acknowledgments.
Incident Response Identification, containment, evidence preservation, investigation, recovery, breach analysis, notification, and lessons learned.	**Disaster Recovery & Backup** Critical-system recovery planning, backup monitoring, restoration testing, and emergency-mode procedures.
Access Lifecycle Authorization, least privilege, MFA where applicable, privileged-access approval, role changes, and termination/offboarding.	**Vendor / BAA Management** Data-flow review, ePHI access determination, BAA status, security review, and periodic vendor reassessment.
Annual HIPAA Review A structured review of risk, access, logging, backups, workforce, vendors, application security, and incident readiness.	**Evidence Register** An index of configuration evidence, reports, signed agreements, training records, test results, and review dates.

Security Officer oversight

ResiCareHealth's governance model assigns responsibility for coordinating security-risk management, security documentation, access review, incident response, and compliance evidence. Security responsibilities are intended to remain active throughout the lifecycle of the platform rather than being treated as a one-time implementation exercise.

03 Technical Safeguards

Layered controls across access, encryption, application operations, and auditability.

Identity and access control

- Access is granted according to legitimate business need and least-privilege principles.
- Privileged or administrative access requires separate approval when appropriate.
- AWS administrative accounts are protected with multi-factor authentication.
- Access changes and terminations are handled through a documented access lifecycle process that includes removal of AWS, database, source repository, deployment, support, email, VPN/remote-access, API-token, and password-manager access as applicable.
- Workforce members are prohibited from sharing passwords, MFA codes, API keys, or other credentials and from accessing customer information without a legitimate business purpose.

Encryption and data protection

ResiCareHealth uses Amazon S3 for object/file storage within its AWS environment. all S3 object uploads are automatically encrypted at rest with server-side encryption using Amazon S3 managed keys (SSE-S3) as the base level of encryption. ResiCareHealth also uses encryption controls for its PostgreSQL production environment.

Transmission-security controls are designed to protect information while moving over electronic networks. ResiCareHealth's evidence program includes verification of HTTPS/TLS configuration and related application-security controls as part of its ongoing security review process.

Application and environment controls

- Production access is restricted to authorized personnel based on role and operational need.
- Role and permission structures are reviewed as part of the company's application-security and annual-review process.
- Customer/tenant separation and API security are included in application-security review activities.
- Production PHI should not be placed into unapproved development or testing tools.
- Credentials and production secrets are prohibited from being embedded in source code.
- Vulnerability findings and remediation are tracked through the risk-management and evidence process.

Defense in depth

No single safeguard is treated as sufficient. ResiCareHealth combines governance, access controls, encryption, logging, backups, workforce requirements, vendor controls, incident response, and evidence review to reduce security risk across the service lifecycle.

04 AWS Cloud Security & Resilience

Cloud infrastructure supported by Amazon S3, AWS CloudTrail, and AWS-native backup capabilities.

Amazon S3 object storage

ResiCareHealth uses Amazon S3 as part of its object/file storage architecture. AWS documents that S3 automatically applies SSE-S3 to new object uploads as the base level of server-side encryption. This provides an AWS-managed encryption baseline for stored S3 objects.[6]

AWS CloudTrail audit visibility

ResiCareHealth uses AWS CloudTrail to support cloud audit logging. AWS describes CloudTrail as a service for operational and risk auditing, governance, and compliance, with actions taken by a user, role, or AWS service recorded as events. CloudTrail events can include activity from the AWS Management Console, AWS CLI, SDKs, and APIs.[7]

Backup and recovery

ResiCareHealth uses AWS-native backup capabilities as part of its data-protection and recovery strategy. AWS Backup is AWS's fully managed service for centralizing and automating data protection across supported AWS services; AWS also provides service-native backup and recovery features.[8] ResiCareHealth's internal Disaster Recovery & Data Backup Plan addresses backup monitoring, restoration testing, recovery responsibilities, and emergency-mode operations.

Cloud shared responsibility

Cloud security is a shared-responsibility model. AWS provides security capabilities for the underlying cloud infrastructure and services, while ResiCareHealth remains responsible for configuring and operating its AWS environment appropriately for its use case. HHS cloud-computing guidance likewise emphasizes that organizations using cloud services remain responsible for HIPAA obligations, appropriate safeguards, and BAAs where required.[4]

AWS / Platform Layer	ResiCareHealth Responsibility	Security Objective
S3 object storage	Appropriate bucket configuration, access permissions, data handling, and review	Protect stored data and limit unauthorized access
CloudTrail	Enable/use audit records and review logging configuration appropriate to risk	Support accountability, investigation, and audit visibility
AWS-native backups	Configure backup scope, frequency, retention, monitoring, and restoration testing	Support availability and recoverability
IAM / administrative access	Least privilege, MFA, access approval, periodic review, offboarding	Reduce risk of unauthorized privileged access

05 Security Operations, Incident Response & Continuity

Prepared processes for detection, containment, investigation, recovery, and follow-through.

Incident response lifecycle

1. Identify Record discovery time, reporter, systems, customer/data impact, and initial severity.	**2. Contain** Limit exposure by disabling accounts, resetting credentials, revoking keys/tokens, isolating systems, or suspending affected integrations when appropriate.
3. Preserve evidence Retain relevant logs, screenshots, system records, emails, and vendor communications before cleanup.	**4. Investigate** Determine what occurred, how it occurred, systems and data affected, whether ePHI was involved, and whether data was viewed, changed, downloaded, or deleted.
5. Eradicate & recover Remove malicious activity, patch vulnerabilities, rotate credentials, restore services, validate integrity, and monitor for recurrence.	**6. Breach analysis** If PHI may have been impermissibly accessed, acquired, used, or disclosed, perform a documented HIPAA breach risk assessment and obtain appropriate privacy/legal review.
7. Notify as required Follow applicable HIPAA and contractual notification obligations.	**8. Correct & learn** Document root cause, corrective actions, owners, due dates, evidence of completion, and lessons learned.

Business continuity and disaster recovery

- Critical systems are identified and prioritized for recovery planning.
- Backup jobs and failures are intended to be monitored and corrected.
- Restoration testing is part of the evidence and annual-review process.
- Recovery objectives are to be based on actual business requirements, architecture, customer commitments, and tested capability rather than assumptions.
- Emergency-mode procedures and recovery contacts are maintained as part of the continuity program.

Breach-response principle

Encryption can materially reduce breach risk, but encryption alone does not eliminate incident-response obligations. ResiCareHealth's breach-assessment process evaluates the nature and extent of PHI, the unauthorized person, whether PHI was actually acquired or viewed, and the extent of mitigation.

06 Workforce, Vendors & Business Associates

Security expectations extend beyond technology to people, contractors, and third-party services.

Workforce security

ResiCareHealth's workforce security program is designed to provide role-appropriate privacy and security awareness to employees, officers, contractors, developers, and other workforce members whose duties involve company systems, PHI, or ePHI. Training topics include PHI/ePHI handling, minimum necessary access, passwords and MFA, phishing and ransomware, secure communications, device and remote-work security, secure handling of customer support files, and incident reporting.

- No unauthorized or curiosity-based access to customer information.
- No credential, password, MFA-code, or API-key sharing.
- No transmission of PHI to personal email accounts.
- No placement of production PHI in unapproved development/test tools.
- Prompt reporting of suspected privacy or security incidents.
- Use only approved systems and access paths for PHI/ePHI.

Vendor and BAA management

ResiCareHealth maintains a vendor/Business Associate Agreement (BAA) review process that evaluates whether a vendor creates, receives, maintains, transmits, or has privileged access capable of reaching ePHI. Security reviews consider encryption, authentication, MFA where relevant, data location/hosting, backup/recovery, incident notification, data return/deletion, subcontractors, and supporting security documentation.

HHS guidance requires a HIPAA-compliant BAA when a cloud service provider creates, receives, maintains, or transmits ePHI on behalf of a covered entity or business associate. HHS also emphasizes that cloud use does not transfer the customer's or business associate's HIPAA obligations to the cloud provider.

Customer responsibilities

A secure SaaS platform still depends on secure customer operation. Customers remain responsible for their own workforce policies, user provisioning, credential hygiene, device security, appropriate access decisions, lawful use and disclosure of PHI, and prompt reporting of suspected incidents. ResiCareHealth recommends that customers:

- Provision access only to authorized users who need it for their job duties.
- Remove user access promptly when employment or responsibilities change.
- Use strong, unique credentials and any available multi-factor authentication features.
- Secure workstations, mobile devices, and local networks used to access the platform.
- Avoid shared user accounts and credential sharing.
- Follow their own HIPAA privacy, minimum-necessary, documentation, and breach-response obligations.
- Contact ResiCareHealth promptly if suspicious access, data exposure, or security concerns are identified.

07 Security Assurance for Prospects

A transparent view of what this white paper does - and does not - establish.

What ResiCareHealth can support during due diligence

This white paper is designed to answer the first level of security and compliance review for prospective customers. Where appropriate and subject to confidentiality and the sensitivity of the requested material, ResiCareHealth's internal compliance package is structured to support requests for information such as:

- Security and privacy policy summaries.
- Security Risk Assessment and risk-management information.
- Business Associate Agreement documentation and vendor/BAA tracking.
- Access-control and termination procedures.
- Incident-response and breach-assessment procedures.
- Disaster recovery and backup procedures.
- Workforce security-training expectations and records.
- AWS configuration evidence, audit/logging evidence, and backup evidence appropriate to the request.
- Annual security-review and compliance-evidence records.

Frequently asked security questions

Is ResiCareHealth "HIPAA certified"? No. HHS does not certify products as "HIPAA compliant." ResiCareHealth maintains a HIPAA-oriented security and privacy program with documented safeguards, risk management, BAAs where required, and implementation evidence.	**Where is object/file data stored?** Amazon S3 is part of the AWS architecture. AWS applies server-side encryption as the base level for new S3 object uploads.
Does ResiCareHealth use cloud audit logging? Yes. AWS CloudTrail supports cloud activity logging and audit visibility.	**Are backups used?** Yes. AWS-native backup capabilities and documented recovery procedures support recoverability.
Is administrative MFA used? Yes. Multi-factor authentication is implemented for AWS administrative access.	**Does ResiCareHealth manage vendor risk?** Yes. Vendor review addresses ePHI access, BAA requirements, encryption, authentication, recovery, incident obligations, subcontractors, and data return/deletion.
Does ResiCareHealth have incident-response procedures? Yes. The process covers identification, containment, evidence preservation, investigation, recovery, breach analysis, notification, corrective action, and lessons learned.	**Does this white paper replace a customer's own HIPAA obligations?** No. Customers remain responsible for their own policies, workforce practices, access decisions, device security, lawful PHI use, and applicable obligations.

08 Authoritative References & Document Notice

Primary federal and AWS sources used to support the statements in this paper.

Federal / regulatory sources

[1] U.S. Department of Health & Human Services - The Security Rule. Official source

[2] U.S. Department of Health & Human Services - Are we required to 'certify' our organization's compliance with the standards?. Official source

[3] U.S. Department of Health & Human Services - Guidance on Risk Analysis. Official source

[4] U.S. Department of Health & Human Services - Guidance on HIPAA & Cloud Computing. Official source

[5] U.S. Department of Health & Human Services - Business Associates. Official source

AWS technical sources

[6] Amazon Web Services - Using server-side encryption with Amazon S3 managed keys (SSE-S3). Official source

[7] Amazon Web Services - What Is AWS CloudTrail?. Official source

[8] Amazon Web Services - What is AWS Backup?. Official source

Internal ResiCareHealth sources

ResiCareHealth HIPAA Compliance Supporting Documents, Version 1.0 (August 12, 2026), including the Security Risk Management Plan; Security Training Policy; Incident Response Plan; Breach Risk Assessment Form; Disaster Recovery & Data Backup Plan; User Access & Termination Checklist; Vendor / BAA Register; Annual HIPAA Compliance Checklist; and HIPAA Compliance Evidence Register.

Document notice

This white paper describes ResiCareHealth's security and privacy program as of August 14, 2026. It is for informational and due-diligence purposes only and is not a warranty, legal opinion, independent audit, SOC 2 report, government certification, or guarantee of any customer's compliance. Controls and services may evolve as the platform and regulatory environment change.

ResiCareHealth LLC | www.resicarehealth.com

Security questions and due-diligence requests may be directed through your ResiCareHealth contact.