REZOLVE.ai

HIPAA Compliance Report

as of April 29, 2025

Risk · Pro

www.riskpro.in

April 29, 2025

To,
The Management,
Rezolve.AI
USA

HIPAA Compliance Report

Scope

Riskpro India was engaged to perform HIPAA Compliance audit for Rezolve.AI services i.e. Rezolve.AI, Morsel.AI, since the company provides products and services for healthcare segment.

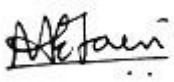
The regulatory scope of this report is limited to Health Insurance Portability and Accountability Act.

Summary Findings / Areas of Concern or Improvement:

- The organization has all the necessary HIPAA specific policies and procedures.
- The organization has identified the scenarios in which it will have access to ePHI. These scenarios are listed in attached annexure. Adequate technical, administrative and physical safeguards are in place to ensure Confidentiality, Integrity and Availability for ePHI.
- The organization has robust Information Security controls. Implementation of retention requirement is in progress.
- Details of current safeguards are in the attached annexure.

Conclusion on HIPAA Compliance

Based on our review and based on the compliance checkpoints outlined in the attached review report, we believe that the organization and its product development is "**HIPAA Compliant**".



Manoj Jain
Director

Disclaimer: This report is intended only for information purpose and should not be considered as an absolute audit report. This is also not a certificate for HIPAA compliance. It is merely an independent review and reporting of our findings to provide assurance to end clients about the HIPAA readiness of our client.

Annexure 1: Scenarios in which Rezolve.AI have access to ePHI:

Rezolve.AI is a leading Virtual Agent (ChatBot) company having products i.e. Rezolve.AI, Morsel.AI. Rezolve.AI have potential access to ePHI in following scenarios:

- **Scenario 1:** The information that Rezolve.AI has access from the Healthcare clients is limited to Employee name, Employee ID, Corporate number, Manager details, Cost centre and Invoices of the client.

- **Scenario 2:** Access to ePHI, the support team may potentially get while resolving issues related to deployment or later on during the support. Rezolve.AI will restrict to members of support team and will have limited control as well as access to ePHI data.

In both of the above scenarios, there is may be some patient medical data such as Patient Health records, Health reports, Health consultations, etc which is created, stored or transmitted through Rezolve.AI products.

Annexure 2: HIPAA Specific Safeguards:

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
Administrative Safeguards	Security Management Process §164.308(a)(1)(i)	Compliant	21-April -2025 • The organization is ISO-27001:2013, SOC 2 Type 2 and GDPR Report certified and maintains comprehensive ISMS documentation. Rezolve.ai is currently in process of migrating to compliance with ISO 27001:2022 standard and hopes to complete the same by May 2025. • Version control is implemented for all policies and procedures. Regular reviews are carried out for policies and procedures. • The organization has a documented risk management policy which also factors Electroninc Heath Information(eHI). • Security leadership is involved in risk management process. • ISMS policies including the ones applicable for data privacy and HIPAA are kept in a shared folder. • Various policies contain examples of unacceptable behavior and other policy violations. HR has policies and procedures deal with violations with various degrees of severity. • Internal audit function has been setup and the scope covers Information systems.
	Assigned Security Responsibility §164.308(a)(2)	Compliant	21-April -2025- • For ISMS Security Officer and his team are responsible for security. • For HIPAA, assignments related to Security and Privacy officer responsibility are listed in HIPAA manual. • The qualifications, experience and job description required for the role have been laid out in the roles and responsibilities document. • An updated formal Org. Chart.
	Workforce Security §164.308(a)(3)(i)	Compliant	21-April -2025 - • The organization has procedures to enable access to employees only to those areas that have been decided upon by the process in which they have been assigned. • Our clients use the application we have developed but we do not have the access to the information stored by those clients either in the storage or application itself.

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
			• Disciplinary policy explicitly states sanctions for violations of policy. • Training is given to the designated persons, who would then train the operators to have sufficient information to carry out their duties. • On termination of a workforce member, the IT department removes all logical and physical access.
	Information Access Management §164.308(a)(4)(i)	Compliant	21-April -2025 - • The organization has procedures to enable access to employees only to those areas that have been decided upon by the process in which they have been assigned. • Defined JDs, and lines of authority for reporting are in place. Responsibilities are defined in procedures manual. • On the job trainings are used to enable the operators to carry out their job functions. • Background verification checks as per process requirement are carried out prior to onboarding. In some cases, based on need, medical checks are performed. • The organization has documented Physical access control policy and logical access control policy We do not have access to the messages customers share and all the msgs are stored in encrypted storage and transmitted in an encrypted channel,
	Security Awareness and Training §164.308(a)(5)(i)	Compliant	21-April -2025- • The Organization is not a covered entity and is likely to be a business associate. • Information security trainings are provided to all new joiners. • The trainings are repeated annually. Effectiveness of the training will be planned and evaluated through a quiz. Results of the evaluations will be maintained. • HIPAA overview training along with ISMS refresher training would be provided to teams such as development, IT Infrastructure staff.
	Security Incident Procedures §164.308(a)(6)(i)	Compliant	21-April -2025 - • The organization has a well-defined incident management process. • Incident logs are maintained for security incidents. • Incident reporting is in the form of tickets raised in JIRA. The tickets also mention timelines, impacts and containment.

	Contingency Plan §164.308(a)(7)(i)	Compliant	21-April -2025 - • The organization has documented backup policy and BC-DR plan. There
Safeguards	**Security Standards**	**Overall Compliance Rating**	**Remarks / Comments**
			are not critical systems which includes ePHI. • Business Continuity and Disaster Recovery procedures are in place. • HIPAA requirement of 'Emergency mode operations' / 'Emergency access' is not applicable. The requirement is to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. - - Since Rezolve.ai team do not maintain any system required for critical business process containing ePHI, this requirement is not applicable.
	Evaluation §164.308(a)(8)	Compliant	21-April -2025 - • The organization conducts and plan annual external VA/PT for IT Infrastructure and products. Remediation is done as per policy for vulnerability management.
	Business Associate Contracts and Other Arrangements §164.308(b)(1)	Compliant	21-April -2025- • Process to ensure adequate safeguards based on the contracts is in place. Physical, technical and administrative safeguards are identified. • Given the risk-based review of its service offerings, BAA with critical supplier like Azure is applicable.
Physical Safeguards	Facility Access Controls §164.310(a)(1)	Compliant	21-April -2025- • The organization has documented Physical and environmental security policy. Appropriate physical security controls such as physical access control using access card, CCTV monitoring, provision of UPS, Diesel generator, appropriate protection for sensitive equipment is in place. • Policy for Physical and Environmental Security describes controls for physical access to sensitive areas.

	Workstation Use & Security §164.310(b) §164.310(c)	Compliant	21-April -2025 - • The organization has documented System and Application Access Control policy. Appropriate Workstation Use & Security controls such as Information Access Restriction, Secure Log-on Procedures and Password Management is in place. • During implementation and support of the products Actionable Science team may have access to PHI. However, in
Safeguards	**Security Standards**	**Overall Compliance Rating**	**Remarks / Comments**
			such cases controls implemented by the client are followed. • Rezolve.ai team is trained in not downloading any ePHI (even if client provides access during support) on local desktops / laptops.
	Device and Media Controls §164.310(d)(1)	Compliant	21-April -2025 - • The organization has policy for device and media handling as well as asset enumeration. • An IT Asset Inventory is maintained. • Data Retention Policy is available. - -Retention policy is based on HIPAA retention requirements as well as contract with the clients. Since no eHI data is known so retention periods will be applicable as per data retention policy

Technical Safeguards	Access Control §164.312(a)(1)	Compliant	21-April -2025 - • The networks have automatic logoff and the OS have automatic lock screens, that require passwords for access when locked • The organization holds / have access to PHI in limited scenarios. The network security for access is adequate and all communications are encrypted. • The identity is mapped to processes on which the user is assigned. Before any change of process is carried out, appropriate authorization has to be taken. • Network logout after specified non- activity, workstation lock requiring re- authentication with passwords after specified duration of non-activity is in place • The organization has an established BC- DR procedure. • The policy for locked screens is applicable to all workstations and laptops.
	Audit Controls §164.312(b)	Compliant	21-April -2025- • Analysis programs are present to log use of the network. Network logs are monitored as per policy for system audit and logging. • The organization has policies for corrective and preventive actions. It is recommended to prepare an audit guideline / checklist based on applicable HIPAA requirements which can be used in such audits.
	Integrity §164.312(c)(1)	Compliant	21-April -2025 - • The organization has robust safeguards to ensure that no data can be accessed by third parties.
Safeguards	**Security Standards**	**Overall Compliance Rating**	**Remarks / Comments**
	Person or Entity Authentication §164.312(d)	Compliant	• The organization has procedure for user registration and robust password management. Log in is through Active Directory. • Procedure to verify that a person or entity seeking access to ePHI is the one claimed needs to be included in one of the policies / procedures. - Neither we have access to that environment and nor any privileges. also Access are protected by token based access implementation. Additionally - no known eHI data to protect.

	Transmission Security §164.312(e)(1)	Compliant	21-April -2025 - • The organization has policy for 'Encryption Management'. The policy includes controls for transferring the data.
Organizational Requirements	Business Associate Contracts and Other Arrangements §164.314(a)(1)	Compliant	21-April -2025 - • When appointed as a business associate, adequate safeguards are taken in physical, technical and administrative areas. • Rezolve.ai hosts and operates its software applications using third party managed services of Azure. There are Subscriptions Agreements in place for the same. • Business Associate agreements is in place for critical supplier like Azure based on the current applicability. However, applicability needs to be assessed periodically based on a Risk based approach and whenever there is a major change in applications.
	Requirements for Group Health Plans §164.314(b)(1)	Not Applicable	21-April -2025 - • Not Applicable.
Policy, procedures and documentation requirements	Documentation §164.316(b)(1)	Compliant	21-April -2025 - • The organization is ISO-27001:2013, SOC 2 Type 2 and GDPR Report certified and maintains elaborate ISMS documentation. It is annually reviewed and is version controlled. Rezolve.ai is currently in process of migrating to compliance with ISO 27001:2022 standard and hopes to complete the same by May 2025. • Procedure for control of documents includes document retention requirement and how the documentation is made available to those persons responsible for implementation • References of applicable HIPAA standards are included in the policies and procedures.

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
			• Disciplinary policy explicitly states sanctions for violations of policy. • Training is given to the designated persons, who would then train the operators to have sufficient information to carry out their duties. • On termination of a workforce member, the IT department removes all logical and physical access.
	Information Access Management §164.308(a)(4)(i)	Compliant	• The organization has procedures to enable access to employees only to those areas that have been decided upon by the process in which they have been assigned. • Defined JDs, and lines of authority for reporting are in place. Responsibilities are defined in procedures manual. • On the job trainings are used to enable the operators to carry out their job functions. • Background verification checks as per process requirement are carried out prior to onboarding. In some cases, based on need, medical checks are performed. • The organization has documented Physical access control policy and logical access control policy • We do not have access to the messages customers share and all the messages are stored in encrypted storage and transmitted in an encrypted channel,
	Security Awareness and Training §164.308(a)(5)(i)	Compliant	• The Organization is not a covered entity and is likely to be a business associate. • Information security trainings are provided to all new joiners. • The trainings are repeated annually. Effectiveness of the training will be planned and evaluated through a quiz. Results of the evaluations will be maintained. • HIPAA overview training along with ISMS refresher training would be provided to teams such as development, IT Infrastructure staff.

	Security Incident Procedures §164.308(a)(6)(i)	Compliant	• The organization has a well-defined incident management process. • Incident logs are maintained for security incidents. • Incident reporting is in the form of tickets raised in JIRA. The tickets also mention timelines, impacts and containment.
	Contingency Plan §164.308(a)(7)(i)	Compliant	• The organization has documented backup policy and BC-DR plan. There

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
			are not critical systems which includes ePHI. Business Continuity and Disaster Recovery procedures are in place. HIPAA requirement of 'Emergency mode operations' / 'Emergency access' is not applicable. The requirement is to establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. - • Since Rezolve.ai team do not maintain any system required for critical business process containing ePHI, this requirement is not applicable.
	Evaluation §164.308(a)(8)	Compliant	• The organization conducts and plan annual external VA/PT for IT Infrastructure and products. Remediation is done as per policy for vulnerability management.
	Business Associate Contracts and Other Arrangements §164.308(b)(1)	Compliant	• The organization has documented Physical and environmental security policy. Appropriate physical security controls such as physical access control using access card, CCTV monitoring, provision of UPS, Diesel generator, appropriate protection for sensitive equipment is in place. • Policy for Physical and Environmental Security describes controls for physical access to sensitive areas.
Physical Safeguards	Facility Access Controls §164.310(a)(1)	Compliant	• The organization has documented Physical and environmental security policy. Appropriate physical security controls such as physical access control using access card, CCTV monitoring, provision of UPS, Diesel generator, appropriate protection for sensitive equipment is in place. • Policy for Physical and Environmental Security describes controls for physical access to sensitive areas.

	Workstation Use & Security §164.310(b) §164.310(c)	Compliant	• The organization has documented System and Application Access Control policy. Appropriate Workstation Use & Security controls such as Information Access Restriction, Secure Log-on Procedures and Password Management is in place. • During implementation and support of the products Actionable Science team may have access to PHI. However, in

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
	Device and Media Controls §164.310(d)(1)	Compliant	• The organization has policy for device and media handling as well as asset enumeration. • An IT Asset Inventory is maintained. • Data Retention Policy is available. Retention policy is based on HIPAA retention requirements as well as contract with the clients.
Technical Safeguards	Access Control §164.312(a)(1)	Compliant	• The networks have automatic logoff and the OS have automatic lock screens, that require passwords for access when locked • The organization holds / have access to PHI in limited scenarios. The network security for access is adequate and all communications are encrypted. • The identity is mapped to processes on which the user is assigned. Before any change of process is carried out, appropriate authorization has to be taken. • Network logout after specified non-activity, workstation lock requiring re-authentication with passwords after specified duration of non-activity is in place • The organization has an established BC-DR procedure. • The policy for locked screens is applicable to all workstations and laptops.
	Audit Controls §164.312(b)	Compliant	• Analysis programs are present to log use of the network. Network logs are monitored as per policy for system audit and logging. • The organization has policies for corrective and preventive actions. It is recommended to prepare an audit guideline / checklist based on applicable HIPAA requirements which can be used in such audits.
	Integrity §164.312(c)(1)	Compliant	• The organization has robust safeguards to ensure that no data can be accessed by third parties.
	Person or Entity Authentication	Compliant	• The organization has procedure for user registration and robust password

Safeguards	Security Standards	Overall Compliance Rating	Remarks / Comments
	§164.312(d)		management. Log in is through Azure Active Directory. • Procedure to verify that a person or entity seeking access to ePHI is the one claimed needs to be included in one of the policies / procedures.
	Transmission Security §164.312(e)(1)	Compliant	• The organization has policy for 'Encryption Management'. The policy includes controls for transferring the data.
Organizational Requirements	Business Associate Contracts and Other Arrangements §164.314(a)(1)	Compliant	• When appointed as a business associate, adequate safeguards are taken in physical, technical and administrative areas. • Rezolve.AI hosts and operates its software applications using third party managed services of Azure. There are Subscriptions Agreements in place for the same. • Business Associate agreements is in place for critical supplier like Azure based on the current applicability. However, applicability needs to be assessed periodically based on a Risk based approach and whenever there is a major change in applications.
	Requirements for Group Health Plans §164.314(b)(1)	Not Applicable	• Not Applicable.
Policy, procedures and documentation requirements	Documentation §164.316(b)(1)	Compliant	• The organization is SOC 2 Type 2 Report certified and maintains elaborate ISMS documentation. It is annually reviewed and is version controlled. • Procedure for control of documents includes document retention requirement and how the documentation is made available to those persons responsible for implementation • References of applicable HIPAA standards are included in the policies and procedures.