Privacy

Version 9

REZOLVE.ai

Document Information

Name of the document	Privacy
Release date	19-Dec-2018
Owned by	Mayank Baghel
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Reviewed and no change
4	02-Dec-2021	Reviewed and no change
5	04-Mar-2022	Updated Document Information
6	07-Mar-2023	Updated 3-Administration
7	24-Sep-2024	Updated Document Information
8	24-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	02-June-2026

Table of Contents

Rezolve.ai is adopting this policy to meet all requirements of Federal and State law relating to the security of personal information including health information HIPAA & the HITECH Act. This policy covers privacy requirements across Rezolve.ai and Rezolve.ai domains.
This will be used by all employees.

1 DEFINITION

Business associate (BA) means a person who, other than in the capacity of a member of Rezolve.ai workforce, or as otherwise provided by HIPAA:

1. On behalf of Rezolve.ai, performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information or any other function or activity regulated by HIPAA; or
2. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, where the provision of the service(s) involves the disclosing individually identifiable health information to the person.
3. Is subjected to HIPAA civil and criminal penalties under the HITECH Act, where certain provisions of the HIPAA Privacy and Security Regulations are applied to business associates.
4. Business associates must comply with the following sections of the Security Regulation:
    1. Administrative safeguards (45 C.F.R. § 164.308)
    2. Physical safeguards (45 C.F.R. § 164.310)
    3. Technical safeguards (45 C.F.R. § 164.312)
    4. Policies and documentation (45 C.F.R. § 164.316)
5. In addition, new security requirements under the HITECH Act that are applicable to covered entities shall also be applicable to business associates.

6. In the case of a business associate that obtains or creates PHI pursuant to a business associate agreement, the business associate is also responsible for ensuring that the agreement complies with the requirements under 45 C.F.R. § 164.504(e). The required provisions of the business associate agreements are now enforceable by HHS as well as by the covered entity. In addition, new privacy requirements under the HITECH Act that are applicable to covered entities shall also be applicable to business associates.

Business Associate Agreements (BAA). The HITECH Act changes applicable to covered entities also apply to business associates – for both privacy and security – and "shall be incorporated into" business associate agreements.

Violations/Breach of BAA. A business associate also has obligations to address known patterns of an activity or practices that constitute a material breach or violation of the BAA.

Direct Liability. For any business associate that violates any applicable privacy or security provision, HIPAA civil and criminal penalties will apply to the business associate in the same manner such provisions apply to a covered entity that violates such provision. Under HITECH rules, business associates are now considered a covered entity.

Covered Entity (CE) means a health care provider, a health plan, or a health care clearing house that is covered by and must comply with the Administrative Simplification provisions of HIPAA. HITECH applies certain provisions of the privacy and security regulations to HIPAA business associates and subjects business associates directly to HIPAA civil and criminal penalties.

De-identification means the process by which protected health information is rendered individually unidentifiable through a determination based upon statistical or scientific methods or through the removal of such identifiers listed below:

1. names;
2. all elements of a street address, city, county, precinct, borough, judicial district, zip code and their equivalent geocode, except for the initial three digits of a zip code;
3. all elements of dates (except year) for dates directly related to the individual (e.g., birth dates, admission/discharge dates, date of death), and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. telephone numbers;

5. fax numbers;
6. Social Security numbers;
7. medical record numbers;
8. health plan beneficiary numbers;
9. account numbers;
10. certificate/license numbers;
11. license plate numbers, vehicle identifiers and serial numbers;

12. device identifiers and serial numbers;
13. Universal Resources Locator (URL) addresses;
14. Internet Protocol (IP) address numbers;
15. biometric identifiers, including finger and voice prints;
16. full face photographic images and comparable images; and
17. any other unique identifying number, characteristic or code (e.g., tribal enrollment card number), except that such ages and elements may be aggregated into a single category of age 90 or older.

Designated record set (Legal Health Record) means record or group of records maintained by or for that includes:

1. the medical records and billing records about patients maintained by or for;
2. the enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for a health plan; or
3. information used, in whole or in part, by or to make decisions about patients.

Disclose means to release, transfer, provide access to, or divulge protected health information outside of.

Health information means any information, whether oral or recorded in any form or medium. Includes demographic and billing information, that is created, developed, received, or maintained by and that relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present, or future payment for the provision of health care to a patient.

Legally designated or personal representative means a person authorized by Federal, State, or Tribal laws to act on behalf of another person. Examples of legally designated or personal representatives include parents, individuals acting pursuant to a power of attorney over health care matters, guardians, executors, and individuals approved by a tribal court or council as having authority to act on behalf of another.

Limited data set means protected health information that excludes the following direct identifiers of the patient or of relatives, employers, or household members of the patient:

1. names;
2. postal address information, other than town or city, state, and zip code;
3. telephone numbers;
4. fax numbers;
5. electronic mail addresses;
6. Social Security numbers;
7. medical record numbers;
8. health plan beneficiary numbers;
9. account numbers;
10. certificate/license numbers;
11. vehicle identifiers and serial numbers, including license plate numbers;
12. device identifiers and serial numbers;
13. web Universal Resources Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. biometric identifiers, including finger and voice prints; and
16. full face photographic images and any comparable images.

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

1. to describe a health-related product or service (or payment for such product or service) that is provided by, including communications about the entities participating in a health care provider network;

2. for treatment of the individual;
3. for case management or care coordination for the individual; or
4. to direct or recommend alternative treatment, therapies, health care providers, or settings of care to the individual.

Marketing includes an arrangement between business associate and another entity whereby business associate discloses protected health information to the other entity in exchange for remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to use that product or service.

Payment means the activities undertaken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care or by a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provisions of benefits under the health plan.

Protected health information (PHI) means individually identifiable health information, including demographic information, in any medium including oral, paper, or electronic, collected from an individual that:

1. is created or received by a health care provider, health plan, employer, or health care clearinghouse;
2. relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care of an individual; and
3. identifies the individual or could reasonably be used to identify the individual.

Protected health information does not include education records covered by Federal law or employment records held by a covered entity in its role as an employer.

Public health generally means public health activities and purposes. This includes disclosures authorized by law to public health authorities for the purposes of preventing or controlling disease, injury, vital events, public health surveillance, investigations, and interventions, of receiving child abuse and neglect purposes, for Food and Drug Administration purposes, to persons who may be at risk of contracting or spreading a disease, and to employers for certain employment-related activities.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary means the Secretary of the Department of Health and Human Services or his or her designee.

Use means the sharing, employment, application, utilization, examination, or analysis of PHI within.

2. Application of this Policy:

This Privacy Policy applies to all employees of Rezolve.ai.

3. Administration:

1. **Privacy Officer**
   Mr. Udaya Bhaskar Reddy is Rezolve.ai's Privacy Officer. The Privacy Officer shall have such duties as may be assigned and as described in the Privacy Officer job description. The Privacy Officer shall have primary responsibility for implementing this Privacy Policy and shall serve as the designated contact person to receive complaints and provide further information about matters covered by the Notice of Privacy Practices.
2. **Workforce Training**
   Rezolve.ai shall have a mandatory privacy training program for its workforce, which for purposes of this Privacy Policy includes all employees, volunteers, students/trainees, and any others working under Rezolve.ai control. This training will emphasize the Privacy Policy and related policies, procedures, processes, and practices; be tailored to various workforce roles; and facilitate compliance with applicable Federal or State law, including HIPAA.
3. **Safeguards**
   Rezolve.ai shall implement appropriate administrative, technical, and physical safeguards to protect the

privacy of patient protected health information (PHI), in compliance with applicable Federal or State law, including HIPAA.

4. **Mitigation**
   Rezolve.ai shall, to the extent practicable, mitigate any known harmful effects from use or disclosure of PHI in violation of applicable laws. Unauthorized use or disclosure of PHI must be reported as required by the BAA.
5. **Prohibition of Intimidation or Retaliatory Acts**
   Rezolve.ai and its workforce/agents may not intimidate, threaten, coerce, discriminate against, or retaliate against patients for lodging complaints or exercising privacy rights under Federal or State law, including HIPAA.
6. **Sanctions for Workforce Members**
   Rezolve.ai shall develop and enforce sanctions for any workforce member who fails to comply with this Privacy Policy or related policies. Sanctions and their dispositions shall be documented.
7. **Policies, Procedures, and Documentation**
   Rezolve.ai shall develop and implement necessary policies, procedures, and systems to ensure this Privacy Policy is effective and in compliance with Federal and State law, including HIPAA.

4. Rights of Patients:

Since Rezolve.ai does not engage in direct health-related services with patients, patient access rights under HIPAA do not apply.

5. Uses and Disclosures of Protected Health Information (PHI):

Rezolve.ai shall use PHI **only as instructed by the Covered Entity (CE)**, except in the following cases:

- **Law Enforcement Activities** – PHI may be disclosed to law enforcement agencies.
- **Court Orders and Warrants** – PHI shall be disclosed in compliance with lawful court orders or similar instruments.

6. Minimum Necessary:

1. **General Limitation**
   Rezolve.ai shall make reasonable efforts to limit the use, disclosure, or request for PHI to the minimum necessary to achieve the intended purpose, in compliance with Federal and State law, including HIPAA.
2. **HITECH Compliance**
   Under HITECH, Rezolve.ai shall use a limited data set (as defined in 164.514(e)(2)) or the minimum necessary PHI to accomplish the purpose. The CE or BA disclosing PHI shall determine what is minimum necessary.

7. Verification of Identity and Authority:

- **Common Sense and Professional Judgment**
  Rezolve.ai will apply common sense and professional judgment when verifying identity or authority of any person requesting access to, or action involving, PHI.
- **Verification Procedures**
  Routine requests may be processed using appropriate documentation (e.g., court orders, law enforcement requests, research authorizations). Otherwise, verification is determined on a case-by-case basis per set criteria.

8. Enforcement – Increased and Tiered Penalties:

Tiered Penalty Structure (Under HIPAA):

- **Unknowing Violations** – $100 to $50,000 per violation, up to $1.5 million annually.
- **Due to Reasonable Cause** – $1,000 to $50,000 per violation, up to $1.5 million annually.
- **Willful Neglect (Corrected within 30 days)** – $10,000 to $50,000 per violation, up to $1.5 million annually.
- **Willful Neglect (Not corrected within 30 days)** – $50,000 per violation, up to $1.5 million annually.

Note: Except in willful neglect cases, no civil penalty will be imposed if the violation is corrected within 30 days.

Important:
The official version of this policy is maintained online. Printed copies are dated and for reference only. Always refer to the online version before relying on printed material.

Note- This policy will be reviewed in **March 2027**. Management may revise it at any time depending on circumstances.

*All documents related to policies and procedures—any reference to **Actionable Science** is as good as **Rezolve.ai**.*