Report By: Scrut Automation Inc.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Compliance Report

Entity Name: BlockSurvey Inc (BlockSurvey)

Assessment Date: October 24, 2025
Report Date: October 31, 2025

1. Executive Summary

This document provides detail report based on NIST Special Publication 800-66 Revision 2 – which provides detail implementation and assessment requirements for implementing HIPAA Security Rule.
The HIPAA audit was conducted to evaluate the organization's compliance with the Health Insurance Portability and Accountability Act (HIPAA) regulations, focusing on privacy, security, and breach notification standards. The audit identified key strengths, including robust policies for safeguarding Protected Health Information (PHI) and a well-established security framework. The organization is committed to implementing these measures promptly to maintain high standards of data protection and regulatory adherence.

The report is divided into following subsections:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational requirements
- Policies and Procedures and Documentation Requirements

2. Audit Methodology

The HIPAA audit methodology is designed to systematically assess the organization's compliance with the Health Insurance Portability and Accountability Act (HIPAA) requirements. The following steps outline the approach used during the audit process:

1. **Audit Planning and Scope Definition**
    - Defined the scope of the audit, including covered entities, business associates, and systems handling Protected Health Information (PHI).
    - Identified applicable HIPAA rules, focusing on Privacy, Security, and Breach Notification standards.
2. **Documentation Review**
    - Collected and reviewed existing policies, procedures, and documentation related to HIPAA compliance.
    - Assessed risk analyses, workforce training records, incident response plans, and Business Associate Agreements (BAAs).
3. **Interviews and Stakeholder Engagement**
    - Conducted interviews with key personnel, including compliance officers, IT staff, and department heads, to understand processes and responsibilities.
    - Engaged with employees to assess awareness of HIPAA regulations and organizational policies.
4. **Technical Assessment**
    - Evaluated physical and technical safeguards for PHI, such as access controls, encryption standards, and system security measures.
    - Performed vulnerability scans and system reviews to identify potential security gaps.
5. **Gap Analysis**
    - Compared current practices against HIPAA regulatory requirements to identify non-compliances, vulnerabilities, or areas for improvement.
    - Prioritized findings based on risk level and impact on PHI protection.
6. **Testing and Validation**
    - Validated the implementation of policies and procedures through random checks, such as verifying access logs, reviewing incident response actions, and testing breach notification processes.

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Security Management Process §164.308(a)(1)	§164.308(a)(1) Implement policies and procedures to prevent, detect, contain, and correct security violations.	Risk Assessment Procedures	Risk Analysis	§164.308(a)(1)(ii)(A) Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	Risk Management Procedure is documented and risk assessment is carried out. **Reference:** "Risk Register"	Compliant
		Risk Management Procedures	Risk Management	§164.308(a)(1)(ii)(B) Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Risk Management Procedure is documented and risk assessment is carried out. **Reference:** "Risk Register"	Compliant
		Sanction Policy	Sanction Policy	§164.308(a)(1)(ii)(C) Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	Entity is not a Covered Entity, However, Disciplinary policy is in place.	Compliant
		Information System Activity Procedures	Information System Activity Review	§164.308(a)(1)(ii)(D) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Application logs and system logs are captured and being reviewed. Accesses are being reviewed on quarterly basis. Incidents are captured in the incident register. **Reference:** "Access Review Records, Incident Register, Log Review Records"	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Assigned Security Responsibility §164.308(a)(2)	§164.308(a)(2) Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Assigned security responsibility documentation	CISO and Privacy Officer Roles and Responsibilities	No Implementation Specifications	Security responsibility is assigned to CISO and Privacy Officer. **Reference:** "Organization Chart"	Compliant
Workforce Security §164.308(a)(3)	§164.308(a)(3)(i) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	Authorization and/or Supervision procedures	Authorization and/or Supervision	§164.308(a)(3)(ii)(A) Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	Access Control Policy is defined and documented.	Compliant
		Workforce Clearance Procedures	Workforce Clearance Procedures	§164.308(a)(3)(ii)(B) Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Access Control Policy is defined and documented.	Compliant
		Employee termination procedures	Termination Procedures	§164.308(a)(3)(ii)(C) Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	Accesses are being revoked on the termination of job or change of job role.	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Information Access Management §164.308(a)(4)	§164.308(a)(4)(i) Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Clearinghouse security policies and procedures	Isolating Healthcare Clearinghouse Function	§164.308(a)(4)(ii)(A) If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Entity does not maintain a clearing house and hence this is not applicable.	Not Applicable
		Access Authorization policies and procedures	Access Authorization	§164.308(a)(4)(ii)(B) Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	Access to platform systems, infrastructure, and cryptographic components is restricted to authorized personnel on a need-to-know basis. Access to PHI data is not applicable, as BlockSurvey operates on a zero-knowledge, end-to-end encrypted model and no ephi is collected in BlockSurvey environment.	Compliant
		Access establishment modification policies and procedures	Access Establishment and Modification	§164.308(a)(4)(ii)(C) Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Access to information assets is being provided on need-to-know basis.	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Security Awareness and Training §164.308(a)(5)	§164.308(a)(5)(i) Implement a security awareness and training program for all members of its workforce (including management).	Security reminder documentation	Security Reminders	§164.308(a)(5)(ii)(A) Periodic security updates.	Information security and Privacy Refresher training is conducted through a GRC Portal at least annually for all the employees. Information security training is given to new employees as a part of induction. **Reference**: "Information Security Awareness Training"	Compliant
		Protection from malicious software procedures	Protection from Malicious Software	§164.308(a)(5)(ii)(B) Procedures for guarding against, detecting, and reporting malicious software.	Information security training is given to new employees through a GRC Portal as a part of induction and on annual basis which includes procedures for guarding against, detecting, and reporting malicious software. Reference: "Information Security Awareness Training"	Compliant
		Log-in monitoring procedures	Log-in monitoring	§164.308(a)(5)(ii)(C) Procedures for monitoring log-in attempts and reporting discrepancies.	Information security training is given to new employees as a part of induction and on annual basis which includes procedures for monitoring log-in attempts and reporting discrepancies. Reference: "Information Security Awareness Training"	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Password management procedures	Password Management	§164.308(a)(5)(ii)(D) Procedures for creating, changing, and safeguarding passwords.	Information security training is given to new employees as a part of induction and on annual basis which includes procedures for creating, changing, and safeguarding password. Reference: "Information Security Awareness Training"	Compliant
Security Incident Procedures §164.308(a)(6)	§164.308(a)(6)(i) Implement policies and procedures to address security incidents.	Incident Response policy and procedure	Response and Reporting	§164.308(a)(6)(ii) Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Process are in place to respond to suspected or known security incidents. Reference: "Incident Management Procedure"	Compliant
Contingency Plan §164.308(a)(7)	§164.308(a)(7)(i) Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	Data backup procedure	Data Backup Plan	§164.308(a)(7)(ii)(A) Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Data Backup is done on a daily basis on GCP and Render.	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Disaster recovery procedure	Disaster Recovery Plan	§164.308(a)(7)(ii)(B) Establish (and implement as needed) procedures to restore any loss of data.	Disaster Recovery Plan is defined and documented.	Compliant
		Emergency mode operation procedure	Emergency Mode Operation Plan	164.308(a)(7)(ii)(C) 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.	Business Continuity Plan is in place.	Compliant
		Testing and revision procedure	Testing and Revision Procedure	§164.308(a)(7)(ii)(D) Implement procedures for periodic testing and revision of contingency plans.	BCP is being tested at least on annual basis. Reference – BCP Test Report	Compliant
		Assessment procedures	Applications and Data Criticality Analysis	§164.308(a)(7)(ii)(E) Assess the relative criticality of specific applications and data in support of other contingency plan components.	BCP is being tested at least on annual basis. Reference – BCP Test Report	Compliant
Evaluation §164.308(a)(8)	§164.308(a)(8) Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Technical and non-technical evaluation procedures	No Implementation Specifications	No Implementation Specifications	Vulnerability Assessment and Penetration Testing (VAPT) is conducted annually.	Compliant

1) Administrative Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Business Associate Contracts and Other Arrangements §164.308(b)	§164.308(b)(1) A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.	Business associate satisfactory associate documentation	Written Contract or Other Arrangement	§164.308(b)(4) Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	There have Business Associate which are GCP and Render Cloud. Entity has GCP and Render Business Associate Addendum (BAA) in place. Note: No PHI is stored on the cloud.	Compliant
2) Physical Safeguards						
Facility Access Controls §164.310(a)	§164.310(a)(1) Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Contingency Operations procedure	Contingency Operations	§164.310(a)(2)(i) Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	Disaster recovery plan is defined and documented.	Not Applicable
		Facility security policy and procedure	Facility Security Plan	§164.310(a)(2)(ii) Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	Policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft are implemented. Reference: "Physical and Environmental Security Policy"	Not Applicable

2) Physical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Access control and validation procedure	Access Control and Validation Procedures	§164.310(a)(2)(iii) Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	Procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision is implemented. Reference: "Physical and Environmental Security Policy"	Not Applicable
		Maintenance records policy and procedure	Maintenance Records	§164.310(a)(2)(iv) Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Policies and procedures to document repairs and modifications to the physical components of a facility which are related to security are implemented. Reference: "Physical and Environmental Security Policy"	Not Applicable
Workstation Use §164.310(b)	§164.310(b) Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	Workstation use policy and procedure	No Implementation Specifications	No Implementation Specifications	Acceptable Usage policy is defined and documented.	Compliant

2) Physical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Workstation Security §164.310(c)	§164.310(c) Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	Physical safeguard implementation procedure	No Implementation Specifications	No Implementation Specifications	Physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users. Reference: "Physical and Environmental Security Policy"	Not Applicable
Device and Media Controls §164.310(d)	§164.310(d)(1) Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	Media disposal policy and procedure	Disposal	§164.310(d)(2)(i) Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	Entity follows the Media Handling and Disposal Policy to ensure secure management of all electronic media. While no ePHI is currently collected or stored due to the platform’s zero-knowledge, end-to-end encrypted design, procedures are in place to securely sanitize or destroy media before reuse or disposal.	Compliant
		Media re-use procedure	Media Re-use	§164.310(d)(2)(ii) Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	Entity follows the Media Handling and Disposal Policy to ensure secure management of all electronic media. While no ePHI is currently collected or stored due to the platform’s zero-knowledge, end-to-end encrypted design, procedures are in place to securely sanitize or destroy media before reuse or disposal.	Compliant

2) Physical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Media accountability procedure	Accountability	§164.310(d)(2)(iii) Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Entity maintains the records of movements of hardware and electronic media.	Compliant
		Data backup and storage procedure	Data Backup and Storage	§164.310(d)(2)(iv) Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	Data Backup is done on a daily basis on GCP and Render.	Compliant

3) Technical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Access Control §164.312(a)	§164.312(a)(1) Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	Unique user identification documentation	Unique User Identification	§164.312(a)(2)(i) Assign a unique name and/or number for identifying and tracking user identity.	Generic ID's are not being used. All the logins are being provided through the unique IDs only.	Compliant
		Emergency access procedures	Emergency Access Procedures	§164.312(a)(2)(ii) Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	Emergency access procedure are in place.	Compliant

3) Technical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Electronic termination procedures	Automatic Logoff	§164.312(a)(2)(iii) Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Sessions are being terminated within defined period of inactivity.	Compliant
		Encryption/Decryption documentation	Encryption and Decryption	§164.312(a)(2)(iv) Implement a mechanism to encrypt and decrypt electronic protected health information.	Data is stored in the Firebase which is encrypted.	Compliant
Audit Controls §164.312(b)	§164.312(b) Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Audit procedures	No Implementation Specifications	No Implementation Specifications	Log monitoring tool like Google Cloud Monitoring etc is configured and all the logs are captured.	Compliant
Integrity §164.312(c)	§164.312(c)(1) Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	EPHI integrity policy and procedure	Mechanism to Authenticate EPHI	§164.312(c)(2) Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Access to ePHI is with limited users on need basis with the help of proper approval mechanism.	Compliant
Person or Entity Authentication §164.312(d)	§164.312(d) Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Person or entity authentication procedure	No Implementation Specifications	No Implementation Specifications	Authentication of the users are being done prior to providing access to systems/information.	Compliant

3) Technical Safeguards						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Transmission Security §164.312(e)	§164.312(e)(1) Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Integrity controls documentation	Integrity Controls	§164.312(e)(2)(i) Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Data in transit is encrypted with TLS 1.3 and access is granted on need basis.	Compliant

4) Organizational Requirements						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Business Associate Contracts and Other Arrangements §164.314(a)	§164.314(a)(1): (i) The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in §164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful— (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.	Business associate contract documentation	Business Associate Contracts	§164.314(a)(2)(i) The contract between a covered entity and a business associate must provide that the business associate will—(A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart; (B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; (C) Report to the covered entity any security incident of which it becomes aware; (D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.	Business associate contracts are in place.	Compliant

4) Organizational Requirements						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
		Other arrangement documentation	Other Arrangements	§164.314(a)(2)(ii) (A) When a covered entity and its business associate are both governmental entities, the covered entity is in compliance with paragraph (a)(1) of this section, if—(1) It enters into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (a)(2)(I) of this section; or (2) Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (a)(2)(I) of this section.	Entity is a private entity whereas this requirement is valid only for government entities. Hence, this is not applicable.	Not Applicable
		Other arrangement documentation	Other Arrangements	(B) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate as specified in § 160.103 of this subchapter to a covered entity, the covered entity may permit the business associate to create, receive, maintain, or transmit electronic protected health information on its behalf to the extent necessary to comply with the legal mandate without meeting the requirements of paragraph (a)(2)(I) of this section	Entity is not required by law to perform any function or activity on behalf of other organization and hence control is not applicable.	Not Applicable

4) Organizational Requirements						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
				provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (a)(2)(ii)(A) of this section, and documents the attempt and the reasons that these assurances cannot be obtained. (C) The covered entity may omit from its other arrangements authorization of the termination of the contract by the covered entity, as required by paragraph (a)(2)(i)(D) of this section if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.		
Requirements for Group Health Plans §164.314(b)	§164.314(b)(1) Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Group health plan documentation	Plan Documents	§164.314(b)(2) The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by § 164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	Entity does not have access to any electronic protected health information, hence this control is not applicable.	Not Applicable

5) Policies, Procedure and Documentation Requirements						
Standards	**Guidelines**	**Criteria**	**Specifications**	**Detailed Guidelines**	**Current Level of Implementation**	**Compliance Status**
Policy and Procedures §164.316(a)	§164.316(a) Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.		No Implementation Specifications	No Implementation Specifications	Information Security policies and procedures are in place.	Compliant
Documentation §164.316(b)	§164.316(b)(1) (i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.		Time Limit	§164.316(b)(2)(i) Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	HIPAA specific policies & procedures are in place.	Compliant
			Availability	§164.316(b)(1) Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	HIPAA specific policies & procedures are in place.	Compliant
			Updates	§164.316(b)(1) Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	HIPAA specific policies & procedures are in place.	Compliant

4. Audit Summary

The HIPAA audit was conducted to evaluate the organization’s compliance with the Health Insurance Portability and Accountability Act (HIPAA), focusing on the Privacy Rule, Security Rule, and Breach Notification Rule. The audit assessed the adequacy of policies, procedures, and controls in place to safeguard Protected Health Information (PHI) and mitigate risks associated with unauthorized access, disclosure, or breaches.

5. Disclaimer

All attempts have been made to provide accurate information. The information provided by the customer is based on evidence provided by infrastructure controlled by the organization. Organisation is advised to implement and periodically check the control processes to ensure secure operation.