



Health Insurance Portability and Accountability Act (HIPAA)

Assessment Report

Entity Name:

Human Edge Advisory Services Pvt Ltd

(Human Edge)


Location:

142, Persepolis Apartment, GD Somani Road, Cuffe Parade, Colaba, Mumbai
400005

Audit Dates: 07th July, 2023

Report Dates: 14th July, 2023

Auditor: Jayshree Dutta

BQC ASSESSMENT PVT. LTD.

Authorised Signatory

BQC Assessment Private Limited



Table of Contents

Executive Summary	3
Audit Methodology	3
Administrative Safeguards	4
1. Security Management Process (§ 164.308(a)(1))	4
2. Assigned Security Responsibility (§ 164.308(a)(2))	6
3. Workforce Security (§ 164.308(a)(3))	6
4. Information Access Management (§ 164.308(a)(4))	7
5. Security Awareness and Training (§ 164.308(a)(5))	7
6. Security Incident Procedures (§ 164.308(a)(6))	9
7. Contingency Plan (§ 164.308(a)(7))	10
8. Evaluation (§ 164.308(a)(8))	11
9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))	12
Physical Safeguards	12
10. Facility Access Controls (§ 164.310(a)(1))	12
11. Workstation Use (§ 164.310(b))	13
12. Workstation Security (§ 164.310(c))	13
13. Device and Media Controls (§ 164.310(d)(1))	14
Technical Safeguards	15
14. Access Control (§ 164.312(a)(1))	15
15. Audit Controls (§ 164.312(b))	16
16. Integrity (§ 164.312(c)(1))	18
17. Person or Entity Authentication (§ 164.312(d))	19
18. Transmission Security (§ 164.312(e)(1))	20
Organizational Requirements	21
19. Business Associate Contracts or Other Arrangements (§164.314(a)(1))	21
Requirements for Group Health Plans (§ 164.314(b)(1))	22
Policies and Procedures and Documentation Requirements	23
21. Policies and Procedures (§ 164.316(a))	23
22. Documentation (§ 164.316(b)(1))	23
Audit Summary	24
Disclaimer	24



Executive Summary

This document provides a detailed report based on NIST Special Publication 800-66 Revision 1 – which provides detailed implementation and assessment requirements for implementing HIPAA Security Rule.

The reports provide detailed status of each requirement and its current status with reference to implementation summary, evidence demonstrated, and auditor opinion.

The report is divided into following subsections:

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

Audit Methodology

The audit methodology included performing the following task:

- An audit plan that covered all the teams within the scope of HIPAA compliance
- Understanding the relevance of HIPAA compliance in the organization
- Assets and their risk assessment process
- Vulnerabilities and their risk treatment process
- Verification of existing policies, procedures and records
- Interview with Personnel including administrators and users
- Verification and testing of technical configuration

Administrative Safeguards

1. Security Management Process (§ 164.308(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Identify Relevant Information Systems	Company maintains an asset master that list all forms of assets used for HIPAA processing.	Asset Register	No deviation noted.
Conduct Risk Assessment	Company has documented asset-by-asset risk assessment where each assets strengths and security weaknesses are documented.	Risk Register	No deviation noted.
Implement a Risk Management Program	Company has identified, documented and track security risks as part of risk management program.	Risk Register	No deviation noted.
Acquire IT Systems and Services	IT infrastructure is in place to provide availability. This includes LAN/WAN and end user processing capability that includes desktops/laptops, besides server infrastructure.	Asset Register	No deviation noted.
Create and deploy Policies and procedure	Operational policies (such as NST – Process Document) and security policies (such as Access Control Policy) in place.	HIPAA Plan and ISMS Policies	No deviation noted.
Develop and Implement a Sanction Policy	Disciplinary Action Process is in place.	Disciplinary Action Process	No deviation noted.
Develop and deploy the information System Activity Review Process	Log Review and Retention Policy in place that demonstrates	Log Review and Retention Policy	No deviation noted.

	generation and review of logs.		
Develop Appropriate Standard Operating Procedure	Standard Operating Procedures for Operations exist.	Standard Operating Procedures	No deviation noted.
Implement the information System Activity review and Audit Process	Log Review and Retention Policy in place that demonstrates generation and review of logs.	Log Review and Retention Policy	No deviation noted.

2. Assigned Security Responsibility (§ 164.308(a)(2))

HIPAA Requirements	Controls Specified by the Organization	Evidence/s	Auditor Opinion
Select a Security Official To Be Assigned Responsibility for HIPAA Security	ISMS Roles and Responsibilities includes ISMS Manager responsibilities	ISMS Roles and Responsibilities include ISMS Manager/CISO responsibilities.	No deviation noted.
Assign and Document the Individual's Responsibility	ISMS Roles and Responsibilities includes ISMS Manager responsibilities	ISMS Roles and Responsibilities include ISMS Manager/CISO Responsibilities.	No deviation noted.

3. Workforce Security (§ 164.308(a)(3))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Implement Procedures for Authorization and/or Supervision	Head of Department decides the individual based on skill/competency and business requirement.	Job Description Access Control Policy	No deviation noted
Establish Clear Job Descriptions and Responsibilities	JDs are defined and documented for each role in organization.	Job Description	No deviation noted
Establish Criteria and Procedures for Hiring and Assigning Tasks	Established criteria in place that includes knowledge, skills and abilities.	Screening Records of 4 Sampled Employees	No deviation noted
Establish a Workforce Clearance Procedure	Workforce clearance procedure involves clearing human resource formalities	HR Manual	No deviation noted.

	with HIPAA training and exam.		
Establish Termination Procedures	Termination procedures involve revocation of access, including communication to customers – whose applications are accessed by employees.	HR Manual – Resignation/Termination Exit Process Checklist	No deviation noted.

4. Information Access Management (§ 164.308(a)(4))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Isolate Healthcare Clearinghouse Functions	Company is not Healthcare Clearinghouse – therefore not applicable	Not Applicable	Not Applicable
Implement Policies and Procedures for Authorizing Access	Supervisor (Manager – Data Processing) supervises access to individual access.	Access Control Policy	No deviation noted.
Implement Policies and Procedures for Access Establishment and Modification	Access Control Policy in place – which is driven by ‘need to know’ principle.	Access Review	No deviation noted.
Evaluate Existing Security Measures Related to Access Controls	Access Control Review is performed annually.	Access Review records	No deviation noted.

5. Security Awareness and Training (§ 164.308(a)(5))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Conduct a Training Needs Assessment	Need Assessment was performed as part of HIPAA Risk assessment/gap analysis. Standard awareness HIPAA training was created, training conducted and exam results	HIPAA Training Material, Exam Results	No deviation noted.

	analyzed.		
Develop and Approve a Training Strategy and a Plan	Coverage of training includes HIPAA/ePHI definitions, as well as responsibilities of the user while handling ePHI.	HIPAA Training Material	No deviation noted.
Protection from Malicious Software; Log-in Monitoring; and Password Management	Every new employee undergoes information security awareness where coverage of malicious software, and password protection are key topics besides other topics. For HIPAA additional training in the form of Dos and DONTs' are documented and presented.	Infosec Employee Awareness presentation	No deviation noted.
Develop Appropriate Awareness and Training Content, Materials, and Methods	Two categories of content are in place. For all new employees there is a standard awareness content, and for personnel who have access to ePHI, additional training content exists.	Infosec Employee Awareness presentation. HIPAA Training Material	No deviation noted.
Implement the Training	Training on HIPAA exists and is implemented.	Training Attendance Sheet & Exam Papers	No deviation noted.
Implement Security Reminders	Organisation receives security updated from OEM – which are documented and tracked with IT infrastructure teams.	VAPT- Vulnerabilities	No deviation noted
Monitor and Evaluate Training Plan	Initial training Plan in place	ISMS Annual Plan – Section on Training	No deviation noted.



6. Security Incident Procedures (§ 164.308(a)(6))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Determine Goals of Incident Response	Documented procedure in place that defines steps to be taken in case of an incident	Incident Management Procedure	No deviation noted.
Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism	Documented roles and responsibilities exist to define the applicable process.	Incident Management Procedure	No deviation noted.
Develop and Implement Procedures to Respond to and Report Security Incidents	Documented roles and responsibilities exist to define the applicable process.	Incident Management Procedure	No deviation noted.
Incorporate Post-Incident Analysis into Updates and Revisions	Incidents are documented, tracked till logical closure including learning from incidents, if any.	Incident Management Procedure related Records	No Deviation noted.

7. Contingency Plan (§ 164.308(a)(7))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Develop Contingency Planning Policy	Contingency Objectives are defined as 48 Hours (2 Business Days) within which Business Continuity Plan from another location needs to be restored.	Business Continuity Plan	No deviation noted.
Conduct an Applications and Data Criticality Analysis	Internet Access is identified as the most critical	Business Continuity Plan	No deviation noted.
Identify Preventive Measures	Preventive controls on site in place. Redundancy exists in the form of people/skills, end user processing infrastructure, and internet connections,	Business Continuity Plan	No deviation noted.
Develop Recovery Strategy	Recovery Strategy for site outage is defined.	Business Continuity Plan	No deviation noted
Data Backup Plan and Disaster Recovery Plan	Not Applicable as the process continues on availability of simple end user infrastructure and internet connectivity.	Business Continuity Plan	No deviation noted
Develop and Implement an Emergency Mode Operation Plan	Business Continuity Plan provides individual tasks that involves movement to alternate location.	Business Continuity Plan	No deviation noted
Testing and Revision Procedure	Business Continuity Plan and its testing process is defined	Business Continuity Plan	No deviation noted.



8. Evaluation (§ 164.308(a)(8))

HIPAA Requirements	Controls Specified by the Organization	Evidence/s	Auditor Opinion
Determine Whether Internal or External Evaluation Is Most Appropriate	External Evaluation has been decided by management	Contract with external consultant to perform HIPAA Assessment	No deviation noted
Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule	Company has ISO 27001 as a framework	ISO 27001 – 2013 certification	No deviation noted
Conduct Evaluation	Organization has a formal audit lifecycle process including audit plan/documentation.	Audit Plan and Report	No deviation noted
Document Results	Audit Findings are documented and tracked for closure.	Audit results	No deviation noted
Repeat Evaluations Periodically	An Annual plan for audit – both external and consultant – in place.	Audit Plan	No deviation noted



9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Identify Entities that Are Business Associates under the HIPAA Security Rule	There is no external Business Associate who have access to ePHI information, therefore this is Not Applicable	Not Applicable	Not Applicable
Written Contract or Other Arrangement	Not Applicable	Not Applicable	Not Applicable
Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements Are Not Being Met	Not Applicable	Not Applicable	Not Applicable
Implement An Arrangement Other than a Business Associate Contract if Reasonable and Appropriate	Not Applicable	Not Applicable	Not Applicable

Physical Safeguards

10. Facility Access Controls (§ 164.310(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Conduct an Analysis of Existing Physical Security Vulnerabilities ⁶¹	Not Applicable	Not Applicable	Not Applicable
Identify Corrective Measures	Not Applicable	Not Applicable	Not Applicable
Develop a Facility Security Plan	Not Applicable	Not Applicable	Not Applicable

Develop Access Control and Validation Procedures	Not Applicable	Not Applicable	Not Applicable
Establish Contingency Operations Procedures	Not Applicable	Not Applicable	Not Applicable
Maintain Maintenance Records	Not Applicable	Not Applicable	Not Applicable

11. Workstation Use (§ 164.310(b))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Identify Workstation Types and Functions or Uses	IT asset inventory is under the ownership of IT infrastructure team.	Asset Register	No deviation noted.
Identify Expected Performance of Each Type of Workstation	Acceptable Usage Policy exists that defines dos and don'ts of all Desktops/Laptops	Acceptable Usage Policy	No deviation noted.
Analyze Physical Surroundings for Physical Attributes	Not Applicable	Not Applicable	Not Applicable

12. Workstation Security (§ 164.310(c))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Identify All Methods of Physical Access to Workstations	Not Applicable	Not Applicable	Not Applicable
Analyze the Risk Associated with Each Type of Access	Not Applicable	Not Applicable	Not Applicable
Identify and Implement Physical Safeguards for	Not Applicable	Not Applicable	Not Applicable

Workstations	Not Applicable	Not Applicable	Not Applicable
--------------	----------------	----------------	----------------

13. Device and Media Controls (§ 164.310(d)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Implement Methods for Final Disposal of EPHI	Company has a media destruction policy that demonstrates intent of secure eWaste.	Media Destruction Policy	No deviation noted.
Develop and Implement Procedures for Reuse of Electronic Media	Current infrastructure used by the client for performing data processing is limited to downloaded files from client provided infrastructure. The content if lost is replaceable from the customer provided file shares.	Physical evidence	No deviation noted.
Maintain Accountability for Hardware and Electronic Media	All Assets are documented and maintained.	ISMS Roles and responsibilities – HOD Responsibility section (Refer ISMS Cross Functional Team - CFT)	No deviation noted
Develop Data Backup and Storage Procedures	Backup Policy in place that covers coverage of all essential infrastructures using de-duplication technology.	Backup Policy	No deviation noted



Technical Safeguards

14. Access Control (§ 164.312(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
4.14.Access Control (§ 164.312(a)(1))			
Analyze Workloads and Operations To Identify the Access Needs of All Users	Access based on need to know is defined, documented, and implemented	Access control policy	No deviation noted
Identify Technical Access Control Capabilities	Access to systems is based on AD authentication managed by a technology team that enforces access security	Access control policy	No deviation noted
Ensure that All System Users Have Been Assigned a Unique Identifier	All users have a unique ID	Access control policy	No deviation noted
Develop Access Control Policy	Access based on need to know is defined, documented, and implemented	Access control policy	No deviation noted
Implement Access Control Procedures Using Selected Hardware and Software	Access to systems is based on AD authentication managed by a technology team that enforces access security. Physical Security controls are implemented using Biometrics System	Access control policy	No deviation noted
Review and Update User Access	Access based on need to know is defined, documented, and implemented. The review is subject to annual access or	Access Control Review Records	No deviation noted

	whenever there is an employee movement.		
Establish an Emergency Access Procedure	Business continuity policy exists that ensure restoration of services and access to individuals identified in the BCP	Business Continuity Plan	No deviation noted
Automatic Logoff and Encryption and Decryption	Local System polices locks out the system within 5 minutes of inactivity	Local System Settings	No deviation noted
Terminate Access if it is No Longer Required	Employee relieving process ensures access termination	Human Resource Communication	No deviation noted

15. Audit Controls (§ 164.312(b))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
4.15.Audit Controls (§ 164.312(b))			
Determine the Activities that Will Be Tracked or Audited	The scope of systems under the scope of log review are limited to Active directory, Office 365 and internet connection. Active Directory logs track the end users and administrator tasks. Users of email (Office 365) are limited to perform restricted communication.	Access Control Policy	No deviation noted
Select the Tools that Will Be Deployed for Auditing and System	Each of the used system – Email – have	Access Control Policy	No deviation noted



Activity Reviews	administrative interfaces managed by a team, which is independent to the team – which is having access to ePHI.		
Develop and Deploy the Information System Activity Review/Audit Policy	Company has acceptable usage policy that defines the process	Acceptable Use Policy	No deviation noted
Develop Appropriate Standard Operating Procedures	Log review and analysis process exist that demonstrates existence of a policy.	Log Review and Analysis	No deviation noted
Implement the Audit/System Activity Review Process	Policy in place – where the analyst – performing the review reports to the human resources manager and the head of department for suitable disciplinary action in case of any security policy violation.	Log Review and Analysis	No deviation noted



16. Integrity (§ 164.312(c)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Identify All Users Who Have Been Authorized to Access EPHI	Users are identified based on their need to know requirement upon approval of the Manager operations.	Access Control Matrix	No deviation noted
Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It	All Company owned applications are hosted inside the premises and access is limited based on network authentication through Active Directory.	Access Control Policy	No deviation noted
Develop the Integrity Policy and Requirements	Acceptable Usage Policy exists that defines user integrity Requirements.	Acceptable Use Policy	No deviation noted
Implement Procedures to Address These Requirements	Access to systems is based on access control. Current systems used for HIPAA processing are designed, implemented and changes controlled.	Access Control Policy	No deviation noted
Implement a Mechanism to Authenticate EPHI	Operational checks and balances are in place to verify the data entry processing requirements that ensure unauthorized modification. Systems storing client provided information ensures information retrievable capability in case of individual disk failure.	Operational – Standard Operating Procedures	No deviation noted

Establish a Monitoring Process To Assess How the Implemented Process Is Working	Log review and analysis process exist that demonstrates existence of a policy.	Log Review and Analysis	No deviation noted
---	--	-------------------------	--------------------

17. Person or Entity Authentication (§ 164.312(d))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Determine Authentication Applicability to Current Systems/Applications	Authentication of an individual is performed for each system by providing a unique user ID and password.	Access Control Policy	No deviation noted
Evaluate Authentication Options Available	Authentication is performed to 'something that a person knows' – a password. In addition access to the site is performed by something that a person is – Finger scan in the biometrics.	Access Control Policy + Password Policy	No deviation noted Due to COVID-19 Physical Access Assessment was done remotely and majority of employees were not in office.
Select and Implement Authentication Option	Authentication is performed to 'something that a person knows' – a password. In addition access to the site is performed by something that a person is – Finger scan in the biometrics.	Access Control Policy + Password Policy	No deviation noted Due to COVID-19 Physical Access Assessment was done remotely and majority of employees were not in office.

18. Transmission Security (§ 164.312(e)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
4.18. Transmission Security (§ 164.312(e)(1))			
Identify Any Possible Unauthorized Sources that May Be Able to Intercept and/or Modify the Information	The systems within scope are hosted in company network – whose access is based on formal authentication. Company systems are not hosted from public network therefore the scope of attacks from external users are non-existent.	Access Control Policy	No deviation noted
Develop and Implement Transmission Security Policy and Procedures	Access to EPHI is provided on client provided applications – from where data is downloaded and processed in another client provided application. The access to these applications are based on formal access control policies.	Access Control Policy	No deviation noted
Implement Integrity Controls	Company has cryptography policy in place that ensures encryption of data in transit.	Cryptography Policy TLS Encryption on email	No deviation noted
Implement Encryption	Company has cryptography policy in place that ensures encryption of data in transit.	Cryptography Policy TLS Encryption on email	No deviation noted



Organizational Requirements

19. Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
4.19.Business Associate Contracts or Other Arrangements (§ 164.314(a)(1))	There are no Business Associate Contracts that gets access to EPHI.	Not Applicable	Not Applicable
Contract Must Provide that Business Associates Adequately Protect EPHI	There are no Business Associate Contracts that gets access to EPHI.	Not Applicable	Not Applicable
Contract Must Provide that Business Associate's Agents Adequately Protect EPHI	Not Applicable	Not Applicable	Not Applicable
Contract Must Provide that Business Associates will Report Security Incidents	Not Applicable	Not Applicable	Not Applicable
Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached	Not Applicable	Not Applicable	Not Applicable
Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements	Not Applicable	Not Applicable	Not Applicable
Other Arrangements for Covered Entities and Business Associates.	Not Applicable	Not Applicable	Not Applicable

20. Requirements for Group Health Plans (§ 164.314(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of EPHI	Company performs data processing work; therefore this requirement is not applicable.	Not Applicable	Not Applicable
Amend Plan Documents of Group Health Plan to Address Adequate Separation	Not Applicable	Not Applicable	Not Applicable
Amend Plan Documents of Group Health Plan to Address Security of EPHI Supplied to Plan Sponsors' Agents and Subcontractors	Not Applicable	Not Applicable	Not Applicable
Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents	Not Applicable	Not Applicable	Not Applicable

Policies and Procedures and Documentation Requirements

21. Policies and Procedures (§ 164.316(a))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Create and Deploy Policies and Procedures Update Documentation of Policy and Procedures	For each area of security operations, the organisation has documented policies and processes. Whenever these documents undergo change they are approved by the respective process owner before deployment.	ISMS Document Master List	No deviation noted

22. Documentation (§ 164.316(b)(1))

HIPAA Requirements	Controls Specified by the Organisation	Evidence/s	Auditor Opinion
Draft, Maintain and Update Required Documentation	For each area of security operations, the organization has documented policies and processes. Whenever these documents undergo change the respective process owner before deployment approves them.	ISMS Document Master List	No deviation noted
Retain Documentation for at Least Six Years	Retention Policy is in place that defines retention and associated deletion process.	Information Retention Policy	No deviation noted
Assure that Documentation is Available to those Responsible for Implementation	Each policy/procedure documents is owned by a department head – who in turn ensure that the policy/procedure is	ISMS Document Master List	No deviation noted



	made available to respective team members – who are associated to security policy/process.		
Update Documentation as Required	Each policy/procedure is subject to annual review or as and when changes take place that impacts security operations.	ISMS Policy	No deviation noted

Audit Summary

We have found satisfactory evidence in the above listed control areas based on audit performed. There are no deviations noted.

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. Company is advised to implement and periodically check the control processes to ensure secure operation.

Jayshree Dutta

Information Security ISO 27001:2013 Lead Auditor