Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Assessment Report

Company Name: Squegg Inc

Location: A 13796 NW 19th St, Pembroke Pines, FL – 33028

Assessment Date: 04th July 2025 to 04th August 2025

Report Date: 04 August 2025

Auditor: Sahil Dubey
Certified Information Systems Auditor® (CISA®)
License Number: 232322528

Sahil Dubey

APPROVED

CONTENTS

1. 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 a detailed status of each requirement and its current status with reference to controls/Implementation summary, evidence demonstrated, and the auditor's opinion.

The report is divided into the following subsections:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organisational requirements

2. AUDIT SCOPE

The scope of the assessment is limited to a business process chosen by SQUEGG INC. All controls associated to this process and their degree of HIPAA compliance are tested and reported in this document. This process has 3 member staff managing operations, wherein they are exposed to Protected Health information (PHI).

3. 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 organisation.
- 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.

4. HIPAA SECURITY RULE STANDARD

HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Controls Specified by the Organisation	Evidences	Auditor Opinion
164.306(a)	Ensure Confidentiality, Integrity and Availability	General Requirement covered by SQUEGG INC	All SQUEGG INC policies and procedures	No exception noted
164.306(b)	Flexibility of Approach	General Requirement covered by SQUEGG INC	All SQUEGG INC policies and procedures	No exception noted
164.306(c)	Standards	General Requirement covered by SQUEGG INC	All SQUEGG INC policies and procedures	No exception noted
164.306(d)	Implementation Specifications	General Requirement covered by SQUEGG INC	All SQUEGG INC policies and procedures	No exception noted

5. ADMINISTRATIVE SAFEGUARDS

164.308(a)(1)(i)	Security Management Process			
164.308(a)(1)(ii)(A)	Risk Analysis	SQUEGG INC has a risk assessment approach that assess risk both by assets and ongoing processes.	HIPAA-Risk Register	No exception noted
164.308(a)(1)(ii)(B)	Risk Management	Each identified risk is communicated to risk owner – who has the responsibility to close.	HIPAA-Risk Register	No exception noted
164.308(a)(1)(ii)(C)	Sanction Policy	Log Review in place that demonstrates generation and review of logs based on incidents.	Policy – Network Security	No exception noted
164.308(a)(1)(ii)(D)	Information System Activity Review	Log Review process is in place based on incident.	Policy – Network Security	No exception noted
164.308(a)(2)	Assigned Security Responsibility			
164.308(a)(3)(i)	Workforce Security			

164.308(a)(3)(ii)(A)	Authorization and/or Supervision	Access control policy is in place that determines the access to information/systems, where the access owner – generally the Supervisor – who approves the access.	Access Control Policy	No exception noted
164.308(a)(3)(ii)(B)	Workforce Clearance Procedure	Workforce clearance procedure involves clearing human resource formalities with HIPAA training.	Manual - Human Resources	No exception noted
164.308(a)(3)(ii)(C)	Termination Procedures	Exit procedures involve revocation of access, that includes revocation of both physical and logical access.	Manual - Human Resources	No exception noted
164.308(a)(4)(i)	Information Access Management			
164.308(a)(4)(ii)(A)	Isolation Health Clearinghouse Functions	The company is not Healthcare Clearinghouse – therefore not applicable	Not Applicable	Not Applicable

164.308(a)(4)(ii)(B)	Access Authorization	Access control policy is in place that determines the access to information/systems, where the access owner – generally the supervisor – who approves the access.	Policy - Access control	No exception noted
164.308(a)(4)(ii)(C)	Access Establishment and Modification	Whenever a new user needs additional access, it is subject to approval by the supervisor	Policy - Access control	No exception noted
164.308(a)(5)(i)	Security Awareness Training			
164.308(a)(5)(ii)(A)	Security Reminders	Organisation receives security updates from email	Email newsletter evidence shown	No exception noted
164.308(a)(5)(ii)(B)	Protection from Malicious Software	Every new employee undergoes Induction/Orientation at the time of joining where coverage of Data security and password	HIPAA Training presentation	No exception noted

		protection are key topics besides other topics. Proprietary Information agreement signed by all employees at the time of joining.		
164.308(a)(5)(ii)(C)	Log-in Monitoring	Every new employee undergoes Induction/Orientation at the time of joining where coverage of Data security and password protection are key topics besides other topics. Proprietary Information agreement signed by all employees at the time of joining.	HIPAA Training presentation	No exception noted
164.308(a)(5)(ii)(D)	Password Management	Every new employee undergoes Induction/Orientation at the time of joining where coverage of Data security and password protection	HIPAA Training presentation	No exception noted

		are key topics besides other topics. Proprietary Information agreement signed by all employees at the time of joining.		
164.308(a)(6)(i)	**Security Incident Procedures**			
164.308(a)(6)(ii)	Response and Reporting	Responsibility is owned by HIPAA Security officer	Procedure – Breach Notification	No exception noted

164.308(a)(7)(i)	Contingency Plan			
164.308(a)(7)(ii)(A)	Data Backup Plan	IT Recovery Plan is in place	Technology restoration plan	No exception noted
164.308(a)(7)(ii)(B)	Disaster Recovery Plan	IT Recovery Plan is in place	Technology restoration plan	No exception noted
164.308(a)(7)(ii)(C)	Emergency Mode Operation Plan	Contingency Objectives defines scope of work that will be performed.	Squegg Inc Business Continuity Management documentation	No exception noted
164.308(a)(7)(ii)(D)	Testing and Revision Procedures	Squegg Inc has an annual plan to perform testing, with	Squegg Inc Business Continuity Management documentation	No exception noted

		next due in April 2026.		
164.308(a)(7)(ii)(E)	Applications and Data Criticality Analysis	No onsite application and data dependency.	Technology restoration plan	No exception noted
164.308(a)(8)	Evaluation			
164.308(b)(1)	Business Associate Contracts and Other Arrangements			
164.308(b)(4)	Written Contract	Not Applicable	Not Applicable	Not Applicable

6. PHYSICAL SAFEGUARDS

164.310 (a)(1)	Facility Access Controls			
164.310(a)(2)(i)	Contingency Operations	Contingency Objectives define scope of work that will be performed.	Squegg Inc Business Continuity Management documentation	No exception noted
164.310(a)(2)(ii)	Facility Security Plan	Documented coverage is in place.	Manual - Physical Security	No exception noted
164.310(a)(2)(iii)	Access Control Validation Procedures	Access control policy is in place that defines	Policy Access Control	No exception noted
164.310(a)(2)(iv)	Maintenance Records	All physical infrastructural changes are	Change management records	No exception noted

		subject to approval.		
164.310(b)	Workstation Use			
164.310(c)	Workstation Security			
164.310(d)(1)	Device and Media Controls			
164.310(d)(2)(i)	Disposal	There is no EPHI storage location in the scope. The desktop that is used to remotely access and perform client specific processing requirement, is secured through media.	Manual – IT Operations – Section – IT Operational Procedures	No exception noted
164.310(d)(2)(ii)	Media Re-use	There is no EPHI storage location in the scope. The desktop that is used to remotely access and perform client specific processing requirement, is secured through media. Due to STPI park regulation, media is always	Manual – IT Operations – Section – IT Operational Procedures	No exception noted

		in The premise. Media Reuse is defined.		
164.310(d)(2)(iii)	Accountability	All Assets are documented and maintained. They are owned by IT	Manual – IT Operations – Section 4 – Scope of Systems under HIPAA Scope. There are three Desktops in the scope of HIPAA.	No exception noted
164.310(d)(2)(iv)	Data Backup and Storage	The backup policy is in place	Manual – IT Operations – Section – IT Operational Procedures – Section on backup	No exception noted

7. TECHNICAL SAFEGUARDS

164.312(a)(1)	Unique User Identification	All users have a unique ID		No exception noted
164.312(a)(2)(i)	Emergency Access Procedure	Access to alternate Location is provided When the Emergency The procedure is invoked	Business Continuity Management	No exception noted
164.312(a)(2)(ii)	Automatic Logoff	End-use devices provide	Desktop configurations	No exception noted

		encryption		
164.312(a)(2)(iii)	Encryption and Decryption	End-use devices provide encryption	Desktop configurations	No exception noted
164.312(a)(2)(iv)	Audit Controls			
164.312(b)	Integrity			
164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	Access Authentication of EPHI system takes place through a two step process. First on Active Directory, and then on client applications.	Policy – Access Control and user specific access control matrix	No exception noted
164.312(c)(2)	Person or Entity Authentication			
164.312(d)	Transmission Security			
164.312(e)(1)	Integrity Controls	End point security is implemented	End point configuration	No exception noted
164.312(e)(2)(i)	Encryption	Desktops are encrypted	Desktop Encryption	No exception noted

8. ORGANIZATIONAL REQUIREMENTS

164.314(a)(1)	Business			

	Associate Contracts or Other Arrangements			
164.314(a)(2)	Business Associate Contracts	Not Applicable	Not Applicable	No exception noted
164.314(b)(1)	Requirements for Group Health Plans			
164.314(b)(2)(i)	Implement Safeguards	Not Applicable	Not Applicable	No exception noted
164.314(b)(2)(ii)	Ensure Adequate Separation	Not Applicable	Not Applicable	No exception noted
164.314(b)(2)(iii)	Ensure Agents Safeguard	Not Applicable	Not Applicable	No exception noted
164.314(b)(2)(iv)	Report Security Incidents	Not Applicable	Not Applicable	No exception noted
164.316(a)	Policies and Procedures			
164.316(b)(1)	Documentation	Operating policies and procedures are in place to support HIPAA that includes user responsibility, HR, Physical Security and IT	Master list of Policies and procedures	No exception noted

		operations		
164.316(b)(2)(i)	Time Limit	Defined as part of the document control. The documents are retained for the 6 years.	Master list of Policies and procedures	No exception noted
164.316(b)(2)(ii)	Availability	End users have the visibility of the Policy – Acceptable Use	Policy – Acceptable Use	No exception noted
164.316(b)(2)(iii)	Updates	Changes to documents are reviewed by the process owner, supported by the HIPAA Security Officer.	Master list of Policies and procedures	No exception noted

9. AUDIT SUMMARY

We have found satisfactory evidence in the above-listed control areas based on the audit performed.

10. DISCLAIMER

All attempts have been made to provide accurate information. The audit evidence and the opinion are based on evidence shown by Squegg Inc.

SahilDubey

Signature

APPROVED