Table 1

IAAA Audit Findings Review Results

Audit Item ID	Condition	Causes	Criteria	Consequences	Corrective Action Plan (IAAA)
Identification					
Iden-4	There is no record that contains all significant events that covers the use and management of user identities as well as authentication information	No presence of administrative dashboard that could manage user identity and authentication information	There should be an Administrator dashboard to handle this	System users wouldn't be able to identify who have logged into the system or to who is using the system	Identification
Iden-5	The accounts present in the system aren't manageable by a specific user.	No administrative dashboard that could manage accounts	There should be an Administrator dashboard to handle this	Anyone can delete/disable a user account inside the system	Identification
Authentication					
Authe-3	More than one user can have the same password	No proper password policy	Each user must have a unique password for their account	If more than one user has the same password, it increases the risk of unauthorized access and login to the other person's account	Authentication & Authorization
Authe-9	No scheduled password changes	No proper password policy	The organization must enforce a password policy for users to change their passwords on a weekly, monthly, or annual basis for improved security	The lack of regular password updates increases the risk of it being compromised or stolen by unauthorized users or hackers	Authentication & Authorization
Authe-15	Users aren't automatically logged off the system after a period of inactivity	Users struggle with remembering their login information, which prevents them from accessing the system	Users must be logged out after a period of inactivity to ensure information security	If an account isn't logged out after a period of inactivity, it increases the risk of unauthorized users accessing the user's account when they are away from their personal computers	Authentication & Authorization
Authorization					
Autho-1	No available user can define and properly handle users' roles, delegate tasks/responsibilities, and grant access rights.	Current users are nurses and ENT doctors. Involved organizations possess the information they need. Appwrite is accessible to technical personnel and allows users to see, update, or delete their personal information, roles, or passwords at any time or location.	*ISO 27002-2002:* Necessary to have available users for defining roles, assigning tasks/responsibilities, and providing access privileges *ISACA G38:* Necessary to set user administration procedures involving daily checks on the administration function	Easily modification of users' access rights from the back-end without anyone's request from the organizations ethical concerns Difficulty in tracking who performed specific actions on user administration Complications in audit logs and investigation	Authorization
Autho-3	No administrator can authorize access rights to EMR users	Lack of guidance or requirements for becoming an Otosopia administrator.	*ISO 27002-2002:* Necessary to have an administrator.	Unrestricted access to sensitive patient data Difficulty in tracking	Authorization

			ISACA G38:	user activity	
		Lack of technical understanding among the process owners who should be given admin roles and their functionality in the system.	Necessary to set user administration procedures involving daily checks on the administration function	Users and technical personnel can intentionally or unintentionally misuse access privileges	
Autho-5	No presence of an administrative user interface (UI)	Lack of a prerequisite guide such as an Access Control Corrective Action Plan for the use cases No administrator user	There should be an administrator user interface included to properly perform the role of a real admin user and other authorization criteria	Deficiency and improper application of identification, authentication, authorization, and accountability solutions	Authorization
Autho-8	No access control policy is being utilized	User requirements from nurses or ENT doctors are considered in the development. Lack of application on authorization models Previous team's objectives for the system did not focus mainly on patient data protection.	*ISACA G38, ISO 27002:2002, HIPAA Privacy Rule Compliance Checklist, and NIST:* Establish an access control policy that outlines roles, responsibilities, and procedures	Leaks and misuse of data Difficulty in tracing actions Reduction of trust Lack of visibility in the system into the changes in user access to data	Authorization
Autho-10	There is no access revocation for non-intended users	Can verify/unverify new user accounts created or block accounts through the back-end server, but cannot grant or prohibit users' access to sensitive data based on their role and school assignment No administrator user interface No administrative dashboard that can compare the number of users from the system to the physical counting of users Lack of appropriateness on user administration processes.	*HIPAA Privacy Rule Compliance Checklist:* there should be proper access revocation procedures for reviewing and modifying access authorization for existing users, especially those non-existing or not already involved users. Also, there should be an access control list	Unauthorized Access Sensitive data being exposed or misused	Authorization
Autho-11	Lack of complete compliance or application to the existing access control model that was adopted.	There is RBAC implemented but still lacking and is present only at the back-end of the system No compliance on attribute-based access control model which is needed for the system	*ISO 27002:2002, Security and privacy in electronic health records:* A systematic literature review, and NIST, there should be proper utilization of RBAC and ABAC, not just from the back-end but, from the Admin UI	Neglected defining of access policies based on attributes such as user location, time of access, and other contextual factors. Roles being too broad or poorly defined	Authorization

Autho-12	There is no access control list compromising the list of users containing their roles and permissions	No proper application for the indication and documentation of changes in user roles and permissions No admin and user interface for the admin	*ISO 27002:2002*: there should be an established application of an access control list so that the target admin can be fully guided in giving authorization using the admin UI	Improper User Authorization Lack of specification on who can access what resources Difficulty in tracking and auditing who has access to what resources	Authorization
Autho-13	No administrator can modify/change the access rights of a user who has changed roles	Not in-system but, present in Appwrite which can be easily modified by the technical personnel without the record of changes	*ISO 27002:2002:* there should be a password policy, an updated access control list, and an access control policy	Inadequate management of user access status and communication with the admin accountable for role/privilege changes. Inadequate quality on the audit log.	Authorization
Autho-14	If a user has left the organization, no administrator can remove the said user's access rights to specific information/protected resources	There is no presence of an intended user who permits, denies, or revokes access to data within the system. Present in Appwrite which may easily be modified by technical personnel without record of changes. No proper utilization of the ABAC model	*ISO 27002:2002:* this audit item must be achieved and there should be an access control list, access control policy, and access control model	Former nurses and doctors retained their access to specific data that can be exposed Inadequate access controls make it difficult to maintain accurate audit trails and track user activities Difficulty of knowing who did what	Authorization
Autho-15	No administrator can provide temporary access rights for a limited period and revoke them at the expiration date	No administrator user Available in Appwrite, a backend server that can be readily modified by technical personnel without a record of changes Authorized users can access patient medical data at any time BYOD is how authorized users can access the desktop system as long as they know their authentication credentials. No restrictions on the system's availability during certain operating hours	*ISO 27002:2002:* Need for a mechanism of terminating an electronic session or automatic logoff after a predetermined time of inactivity Data access should be limited to specific times during the day, week, month, or year Access to the system should be during certain operating hours to automatically log users out of the system after the operational hours. There should only be one device per user, and the system should identify pr detect it Administrative safeguards should be in place to prevent patients' data from	Prone to unauthorized access under many circumstances, such as data sharing Prone to data modification from the doctor or data sharing without the presence or agreement of the student involved. Lack of audit trail quality	Authorization

			being transferred off-site		
Accountability					
Acc-1	No audit logs present in the system but only inside the open database accessible to anyone	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the changes made in the system specifically if errors have occurred	Accountability
Acc- 2	Since there is no audit logs, user IDs are not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the user IDs in the system specifically if errors have occurred	Accountability
Acc- 3	Since there is no audit logs, user actions are not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the user actions in the system specifically if errors have occurred	Accountability
Add- 4	Since there is no audit logs, date and time of of a user's log in or system activity are not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the date and time of of a user's log in or system activity in the system specifically if errors have occurred	Accountability
Acc- 5	Since there is no audit logs, specific device / terminal used to perform a user actions are not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the specific device / terminal used to perform a user actions in the system specifically if errors have occurred	Accountability
Acc- 6	Since there is no audit logs, successful and rejected indicators of user actions are not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the successful and rejected indicators of a user actions in the system specifically if errors have occurred	Accountability
Acc- 7	Since there is no audit logs, the affected resource of a specific user's action is not taken to account or recorded	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the the affected resource of a specific user action in the system specifically if errors have occurred	Accountability
Acc-8	With the absence of audit logs, admin user cannot tamper audit log records.	No admin could tamper logs	There should be an Admin user, however, tampering should not be considered in logs.	Without an Admin, no one can track user logs	Accountability
Acc- 9	There is no administrator in the sytem and there is also no administrator dashboard present in the system. The act of deleting logs is not present in the system.	No administrator dashboard that could manage, record, and view an audit logs	There should be a feature in the system or in an admin dashboard for an audit logs to keep track of the changes made in the system	It would be hard to keep track of the Admin changes made in the system specifically if errors have occurred	Accountability

Acc- 10	There currently is no administrator in the system so no admin actions are to be recorded	No administrator assigned/ identified	There should be a system administrator	No specific individual could be assigned for the audit logs	Accountability
Acc- 11	There currently is no audit logs in the system except for the one in the open database of the system that is accessible to anyone, thus other features to analyze the audit log for unusual activities or anomalous behaviour is not recorded	No audit logs in the system itself	There should be an audit logs as well as an administrative dashboard to keep record of system logs	It would be hard to keep track of the other features to analyze the audit log for unusual activities or anomalous behaviour in the system specifically if errors have occurred	Accountability
Acc- 12	There currently is no audit logs in the system that records the "before" and "after" versions of a document	No audit logs in the system itself	There should be an audit logs as well as an administrative dashboard to keep record of system logs	It would be hard to keep track of the records the "before" and "after" versions of a document in the system specifically if errors have occurred	Accountability
Acc- 13	There currently is no audit logs in the system thus log system failure is not recorded	No audit logs in the system itself	There should be an audit logs as well as an administrative dashboard to keep record of system logs	It would be hard to keep track of the log system failure in the system specifically if errors have occurred	Accountability