Table 2

Corrective Action Plans per IAAA Component

Identification	
Risk ID	R-1
Corrective Action ID	CA-1
Risk (Threat / Vulnerability)	High
Action Priority	High
Selected Planned Controls	An administrative UI/ dashboard should be created for an assigned admin.
Description	• Admin list of system users UI • Admin authorization UI • Admin authentication UI • Admin audit log UI • Admin create new user • Admin delete user
Required Resources	Software resources
Accountability	
Risk ID	R-2, R-3
Corrective Action ID	CA-2
Risk (Threat / Vulnerability)	High
Action Priority	High
Selected Planned Controls	Specific changes made in the system in a specific affected resource should be recorded through audit log implementation, as well as to make it available for review by authorized users.
Description	Audit log composed of: ● User access time ● User access date ● User name/identification ● User activity ● User affected resource for change ● Success and rejected indication for log in ● Device identity
Required Resources	Software resources
Authentication	
Risk ID	R-6
Corrective Action ID	CA-3
Risk (Threat / Vulnerability)	High
Action Priority	High
Selected Planned Controls	Forced re-authentication / Automatic log-off
Description	A functionality in the system which allows the future IAM administrator to configure the idle session timeout (in minutes) with the following options: ● 15 minutes ● 30 minutes
Required Resources	Otoscopia's system documentation
Risk ID	R-7
Corrective Action ID	CA-4
Risk (Threat / Vulnerability)	Medium
Action Priority	High
Selected Planned Controls	Forced password change
Description	Functionalities in the system which allows the future IAM administrator to perform the

	following: ● Select password expiration duration ● Select password expiration grace period ● View the final password expiration date Options for the password expiration duration include: ● 60 days ● 90 days ● 180 days ● 270 days ● 365 days (1 year) Options for the password expiration grace period include: ● 1 day ● 2 days ● 3 days ● 4 days ● 5 days ● 6 days ● 7 days (1 week)
Required Resources	Otoscopia's system documentation
Authorization	
Risk ID	R-8, R-9, R-10,R-11
Corrective Action ID	CA-5
Risk (Threat / Vulnerability)	Medium to High
Action Priority	High
Selected Planned Control	Creation of an administrative user interface (UI) that will cater to the authorization functionalities
Description	A user with administrative privileges has the following responsibilities: ● Role Management ● User Account Management (e.g. activation or deactivation of either temporary or non-temporary user accounts) ● Identity Collections Management ● Approval Workflows Management (activation, modification, disablement, and removal of user accounts) ● User's Access Privileges Management ● Authorization Management (e.g. location tracker of users having authorized access to electronically protected health information) ● Information Access Management ● Access Review Management **Admin User's Dashboard Privilege:** ● Includes a summary report on the dashboard about other users' access and activities ● Dashboard is set as the landing page;
Required Resources	● Digital Ocean subscription ● Final adoption of the access control policy based on previous system documentation
Risk ID	R-10
Corrective Action ID	CA-6
Risk (Threat / Vulnerability)	High
Action Priority	High
Selected Planned Controls	Access Control List
Description	A table format listing the permissions associated with the electronic medical records and storing the privileges assigned to users with specifications on the control type of operations, such as 'read', 'create', 'update', and 'delete'.
Required Resources	● Previous documentation about the EMR System ● Audit of the EMR system
Risk ID	R-8, R-10, R-11

Corrective Action ID	CA-7
Risk (Threat / Vulnerability)	Medium to High
Action Priority	High
Selected Planned Controls	Adapt Access Control Policy and Procedures based on *Role-based Access Control (RBAC)* and *Attribute-Based Access Control (ABAC)*
Description	Address compliance procedures based on RBAC and ABAC, as well as user account management procedures **Implementation of Policy and Procedures must consider the following:** ● Protection of transmitted electronic health information from improper modification, alteration, or destruction without detection until disposed of; ● Maintenance of access only to those persons who have been granted access rights; and ● Conditions for disabling or deactivating accounts, including when individuals are transferred or terminated. *Role-based Access Control* ● Authorizing access only when such access is appropriate based on the user's role or healthcare functions; ● Allowing request and approval processes for changes in user assignments; ● Setting roles and role restrictions/interactions; and ● Determining access requirements based on what roles need to be created and what information needs to be associated with which role. *RBAC considers the following:* ● Role Definition ● Role assignment ● Permission assignment ● Role-based provisioning ● Regular reviews and audits *ABAC considers the following:* ● Classification of subject; ● Classification of objects; ● Classification of environmental conditions; ● Classification of attributes for subjects, objects, and environmental conditions;
Required Resources	● Previous documentation about the EMR System ● Audit of the EMR system