Toronto General Hospital Access and Identity Management Solution

Breanna West and Roshan Ramamoorthi

Sheridan College

SYST 32288 - Access and Identity Management

Ali Owayid

April 4th, 2026

Table of Contents

Executive Summary

Overview

Toronto General Hospital is interested in an identity and access management solution to improve access controls and reduce IAM related expenses. The current IAM infrastructure is run on-premise with one IT admin in charge. A new cloud based IAM will address authentication, authorization, identity management and compliance requirements of a public health organization. HIPAA compliance must be ensured throughout the migration to safeguard patient information. The specific scenario used is fictitious; however this proposal provides a realistic overview of how a public health organization would adopt a cloud based identity and access management system.

The IAM solution needs to address the access controls applicable to all roles present in a hospital setting. Some roles would include physicians, nurses, specialists, surgeons, assistants, administrative positions, general staff and more. Each of these roles should only have access to which they need to complete their job and nothing more, ensuring the principle of least privilege. In addition to roles, the hospital can integrate the shift schedule of all workers to improve their security posture. By restricting login access to those that are currently working, any chance of credential misuse or abuse can be mitigated. Hospital operations and processes will be reviewed to ensure separation of duties. This is important so that drug dispensing is done ethically and responsibly.

Key Objectives

- Identity Management
    - Employee Onboarding/Offboarding
    - Maintaining accounts (Password resets, Requesting access)
    - Auditing for orphaned accounts and permission sprawl
- Authentication
    - Multi-Factor Authentication
        - Passwords, Ubi-Key, Fingerprint

    - Zero Trust Policy
- Authorization
    - Role-based access control
        - Doctors have access to only their own patient's data
        - Nurses have temporary access to applicable patients in their ward
        - Temporary access for specialists who periodically visit the hospital
        - Least privilege and just in time access for IT Admins
    - Attribute-based access control
        - Access policies will check for login location, device type, software platform, network configuration
    - Principle of least privilege
        - Roles are only given access to what they need to complete their jobs
    - Separation of duties
        - Critical tasks are divided among multiple individuals to prevent abuse or error
- Audit and Compliance
    - Ensure HIPAA Compliance

Project Background

Scenario Description

Toronto General Hospital recently suffered a cyberattack through an orphaned account. The attack exposed sensitive patient data which pressured a change for a better IAM solution. The account used in the attack was a nurse who was terminated for diverting medications for personal use. The nurse was able to prescribe and withdraw drugs due to a lack of separation of duties. The terminated nurse returned unnoticed and took advantage of their orphaned credentials to expose confidential patient files. This resulted in a HIPAA violation which cost the hospital millions of dollars in fines. The

hospital is now in the process of restructuring their identity and access management system to meet HIPAA compliance.

Research

To address the concerns of the given scenario, a new IAM solution will be formulated using the concepts discussed in class material. Starting with a theoretical analysis of the existing hospital IAM to set expectations of the new cloud based IAM. Accounts should be audited for privilege sprawl and instances of orphaned accounts. After cleaning the existing directory, groups and roles can be formulated to best serve the hospital and IT administration. These roles and groups will serve the foundation to the authorization portion of the IAM solution.

Authentication is important to ensure the user is actually who they claim to be. By default all users will require multi-factor authentication across the board as the IAM solution adopts a zero trust policy. The main factor will be passwords for computers and 6-digit pins for locked doors. The second factor will be a photo identification key card which can be used with RFID scanners for doors and computers. Additional factors such as one time passcode SMS and applicable biometrics will be available as secondary factors. The first two main factors rely on knowledge-based and property based authentications, this approach is scalable for the hospital. Biometrics will be used in areas where the access pool is shallow, allowing for biological-based authentication. Finally SMS codes will be used in addition to passwords for online portals.

Role based access control and Attribute based access control will play a major role in the authorization process. With RBAC, all employees will have pre-defined roles that determine their base permissions. Doctors will have assigned permissions based on their roles such as specialist or full time shift doctors. Working alongside RBAC is attribute based access control, this handles departments, location of employee sign in and time of day. This will affect their access to confidential patient files while on and off site or on shift versus off shift. A nurse will only be able to view patient charts that are assigned to them and doctors may only access records while on shift.

HIPPA requires unique ID, authentication and mitigation of orphaned accounts. This will all be taken care of by the implemented IAM solutions. These are addressed

through automated provisioning and deprovisioning and continuous monitoring for inactive accounts.

This new IAM solution will also enforce the principle of least privilege ensuring each user only receives the minimum access necessary to perform their duties. This will prevent users from being granted unnecessary permissions and reduce the impact of compromised accounts.

Separation of duties will also be incorporated to prevent any single employee from performing any conflicting actions. Prescribing medication will be only allowed by doctors while dispensing and administering medications will fall to nurses and other required staff. This way no employee can finish the work procedure alone, reducing opportunities for fraud and unauthorized access.

Project Design

Chosen System

The system required for Toronto General Hospital must be flexible and highly efficient to serve thousands of employees. There are many IAM solutions available on the market that cater to the needs of a large data sensitive organization. Some of the candidates are Okta, Microsoft Entra ID, Google Cloud and Cisco Duo. All these platforms provide IAM services with competitive features, each with their own strengths and weaknesses.

Service	Strengths	Weaknesses
Okta	• Pre-built Integrations and Lifecycle Management • No credit card for demo	• Premium price point in comparison to competitors
Microsoft Entra ID	• Conditional Access and Microsoft 365 • Access to suite of enterprise Microsoft productivity apps	• Less ideal for integrations across multiple cloud providers • Requires credit card for demo
Google Cloud Identity	• Ease of use and Google Workspaces • Access to Google productivity apps	• Less ideal for Windows based integrations • Requires credit card for demo
Cisco Duo	• Strong MFA and easy deployment • No credit card for demo	• Not a standalone Identity provider

Ultimately Okta was the chosen system due to the extensive lifecycle management tools which is critical to the goals of the cloud migration. These tools will ensure that identities are kept up to date and not abused. Okta will be able to provision, manage and deprovision identities as needed to prevent orphaned accounts and permission sprawl. The platform offers policy rules to enforce attribute-based and role-based access control. The nature of a hospital organization also requires mandatory access control to ensure only the applicable physicians have access to their own patients and no one else.

Project Plan

1. Provisioning Identities
    a. Using the CSV import template offered by Okta, fill in all staff employed at the hospital.
    b. After import check for errors and address
    c. Create groups for the identities based on their roles and department
2. Create Applications
    a. Patient Data Portal
        i. Accessible by Doctors and Administrator
    b. Prescription Order Portal
        i. Accessible by Doctors
    c. Prescription Dispenser
        i. Accessible by Nurses
    d. TimeSheet
        i. Accessible by everyone
    e. Clinical Communication
        i. Accessible by everyone
    f. Patient Imaging
        i. Accessible by Doctors, Surgeons, Administrative Users
    g. Test Application Accessibility and Permissions
3. Create Login Polices
    a. Create a catch all policy applicable to all identities hospital wide

   i. Limit all authentications within the hospital network
   ii. MFA must be used for all authentications
   iii. Device health check before approving authentication
2. Application specific policies to limit their use to authorized personnel
3. Automatic identity lifecycle management to deactivate unused accounts
4. Behaviour detection policies to alert any anomalies for authentication

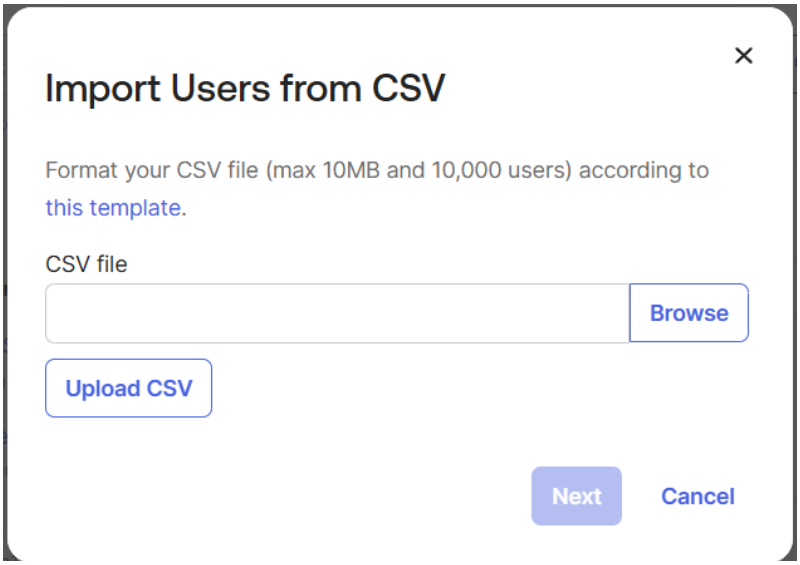
Implementation

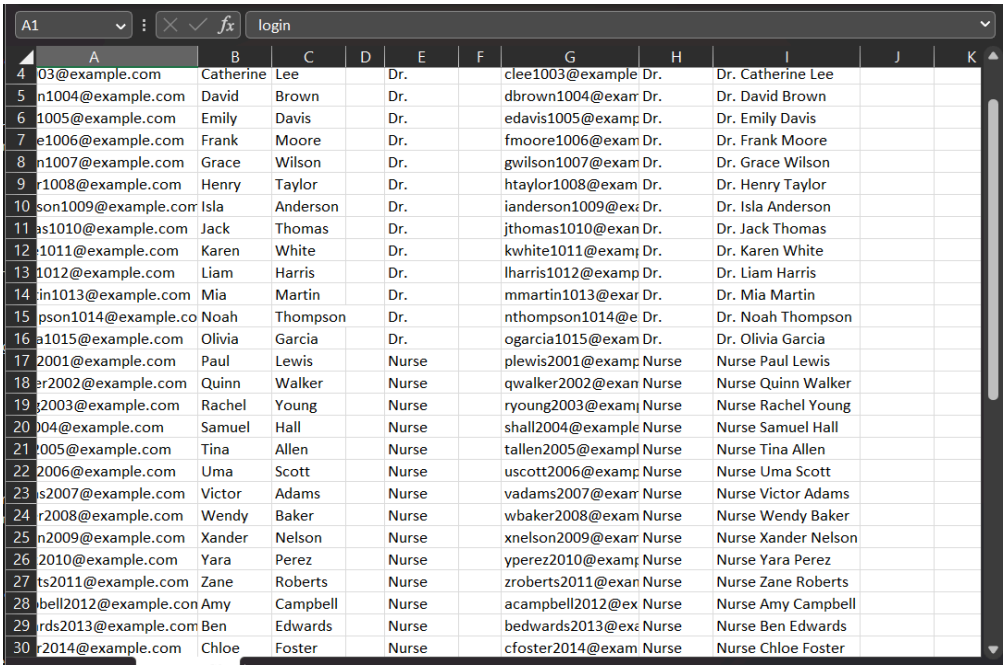
Setup Details

All of the IAM solutions reviewed for this proposal require a credit card except for Okta which made the initial setup process smooth. Using our existing Okta accounts we were able to begin creating the Toronto General Hospital IAM Solution. The solution began with the provision of identities followed by the creation of apps for common hospital services and tools. Finally, access policies were put in place to secure the solution of vulnerabilities.

Configurations Performed

User Provisioning



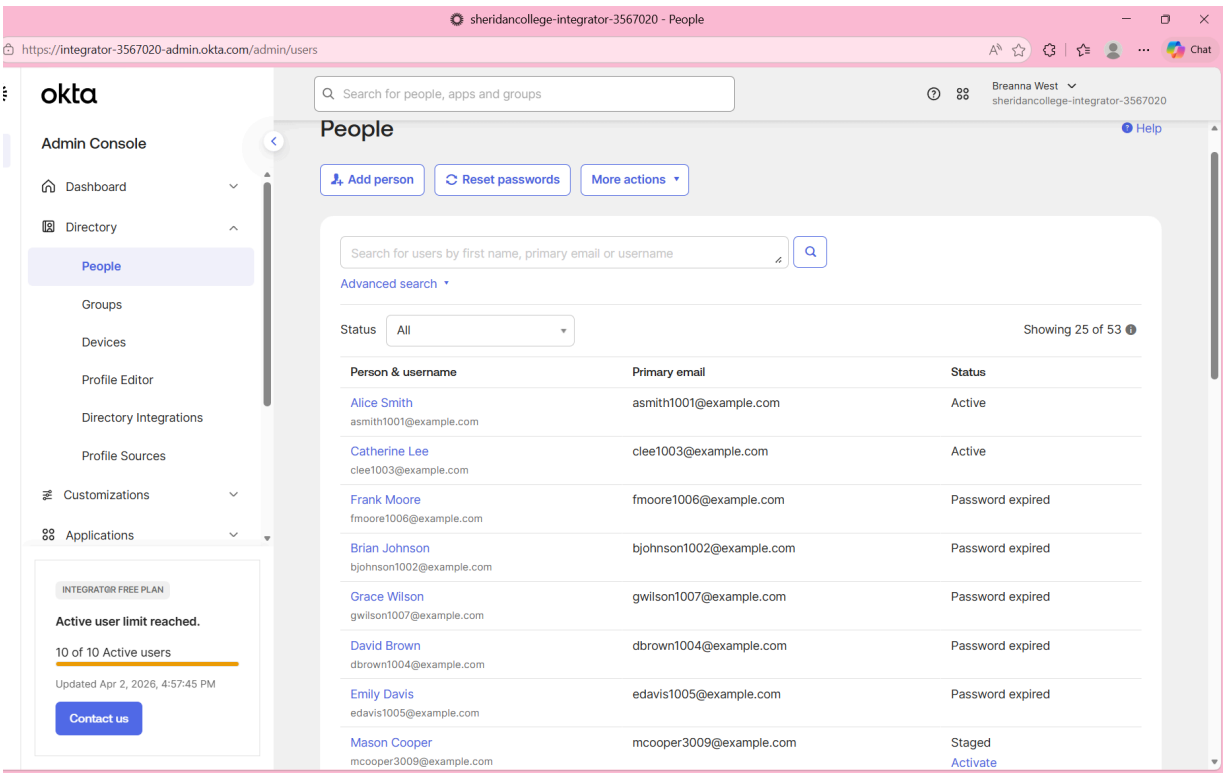


A1 | login

	A	B	C	D	E	F	G	H	I	J	K
4	03@example.com	Catherine	Lee		Dr.		clee1003@example	Dr.	Dr. Catherine Lee		
5	n1004@example.com	David	Brown		Dr.		dbrown1004@exam	Dr.	Dr. David Brown		
6	1005@example.com	Emily	Davis		Dr.		edavis1005@examp	Dr.	Dr. Emily Davis		
7	e1006@example.com	Frank	Moore		Dr.		fmoore1006@exam	Dr.	Dr. Frank Moore		
8	n1007@example.com	Grace	Wilson		Dr.		gwilson1007@exam	Dr.	Dr. Grace Wilson		
9	r1008@example.com	Henry	Taylor		Dr.		htaylor1008@exam	Dr.	Dr. Henry Taylor		
10	son1009@example.com	Isla	Anderson		Dr.		ianderson1009@exa	Dr.	Dr. Isla Anderson		
11	s1010@example.com	Jack	Thomas		Dr.		jthomas1010@exan	Dr.	Dr. Jack Thomas		
12	1011@example.com	Karen	White		Dr.		kwhite1011@examp	Dr.	Dr. Karen White		
13	1012@example.com	Liam	Harris		Dr.		lharris1012@examp	Dr.	Dr. Liam Harris		
14	in1013@example.com	Mia	Martin		Dr.		mmartin1013@exar	Dr.	Dr. Mia Martin		
15	pson1014@example.co	Noah	Thompson		Dr.		nthompson1014@e	Dr.	Dr. Noah Thompson		
16	a1015@example.com	Olivia	Garcia		Dr.		ogarcia1015@exam	Dr.	Dr. Olivia Garcia		
17	2001@example.com	Paul	Lewis		Nurse		plewis2001@examp	Nurse	Nurse Paul Lewis		
18	r2002@example.com	Quinn	Walker		Nurse		qwalker2002@exan	Nurse	Nurse Quinn Walker		
19	2003@example.com	Rachel	Young		Nurse		ryoung2003@exam	Nurse	Nurse Rachel Young		
20	004@example.com	Samuel	Hall		Nurse		shall2004@example	Nurse	Nurse Samuel Hall		
21	005@example.com	Tina	Allen		Nurse		tallen2005@exampl	Nurse	Nurse Tina Allen		
22	2006@example.com	Uma	Scott		Nurse		uscott2006@examp	Nurse	Nurse Uma Scott		
23	s2007@example.com	Victor	Adams		Nurse		vadams2007@exam	Nurse	Nurse Victor Adams		
24	r2008@example.com	Wendy	Baker		Nurse		wbaker2008@exam	Nurse	Nurse Wendy Baker		
25	n2009@example.com	Xander	Nelson		Nurse		xnelson2009@exam	Nurse	Nurse Xander Nelson		
26	2010@example.com	Yara	Perez		Nurse		yperez2010@examp	Nurse	Nurse Yara Perez		
27	ts2011@example.com	Zane	Roberts		Nurse		zroberts2011@exan	Nurse	Nurse Zane Roberts		
28	bell2012@example.com	Amy	Campbell		Nurse		acampbell2012@ex	Nurse	Nurse Amy Campbell		
29	rds2013@example.com	Ben	Edwards		Nurse		bedwards2013@exa	Nurse	Nurse Ben Edwards		
30	r2014@example.com	Chloe	Foster		Nurse		cfoster2014@exam	Nurse	Nurse Chloe Foster		

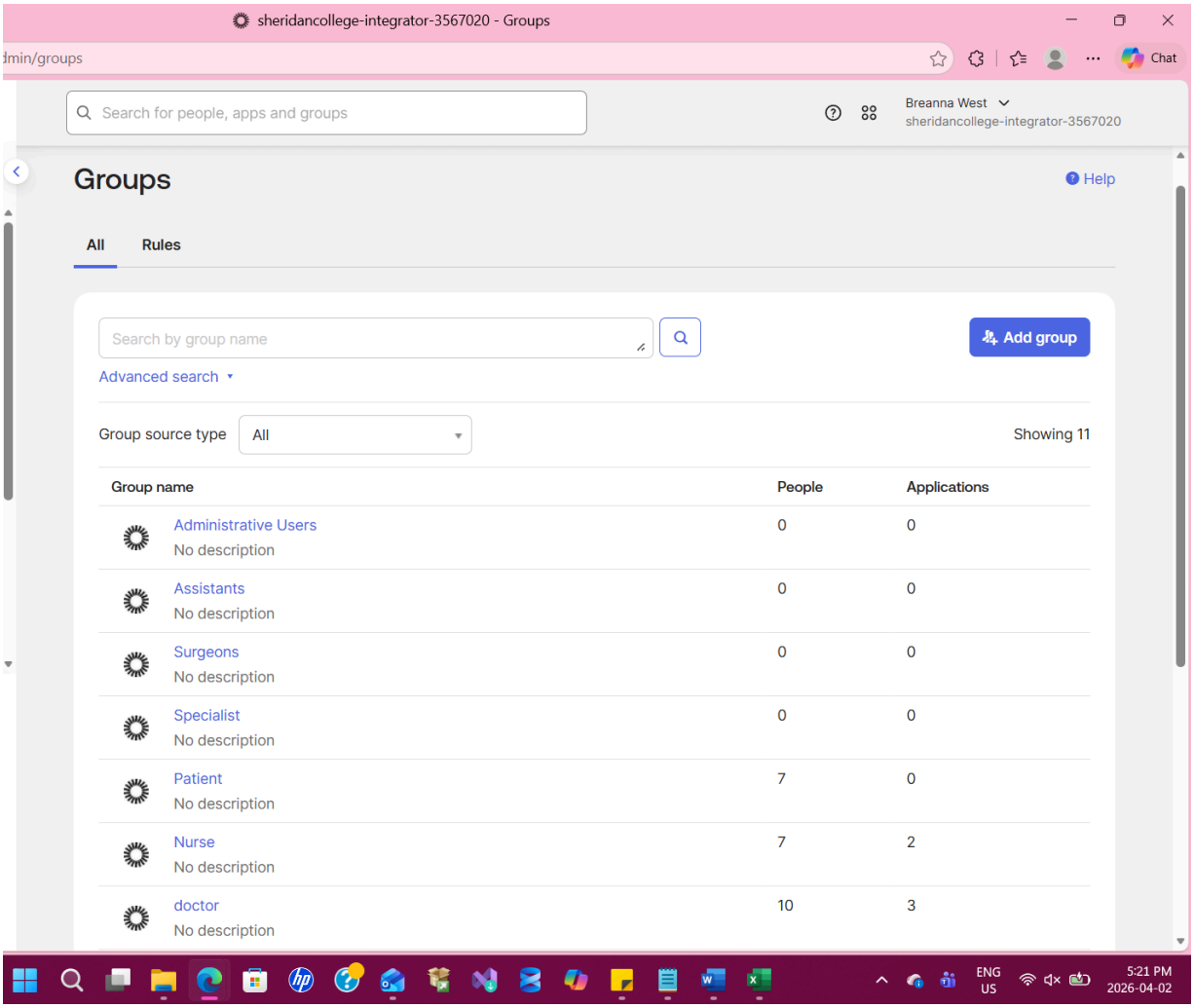
Downloaded the template excel sheet from Okta and filled in 50 users with different names, roles, departments, and emails. Exported the file as a CSV and uploaded the data for easy account provision of 50 users at once.

Okta Active User Limit



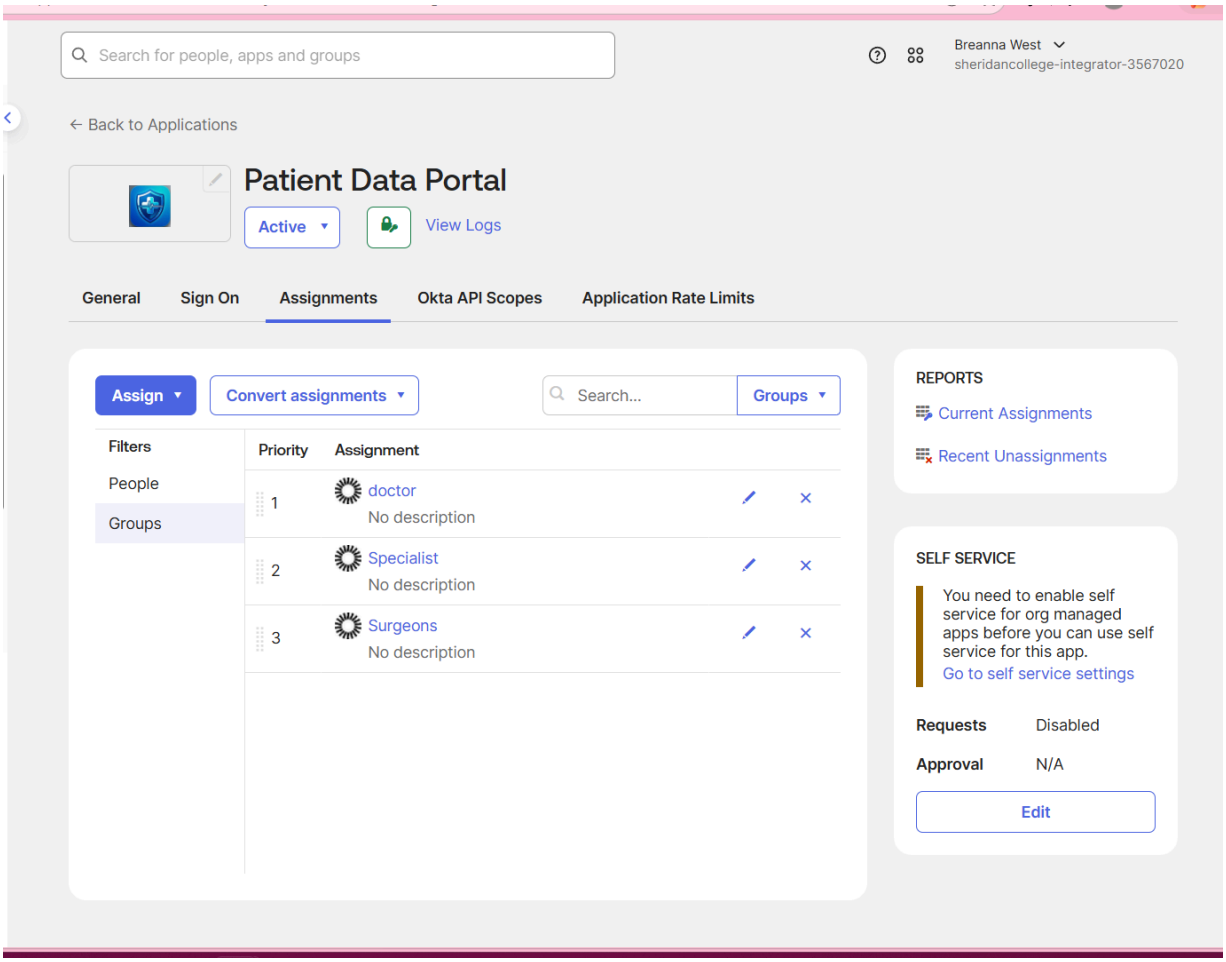
Unfortunately the demo version of Okta only allows 10 active users at a time which limited some of the testing we were able to do but the users could still be organized into groups for easy access control configuration.

Employee Role Groups



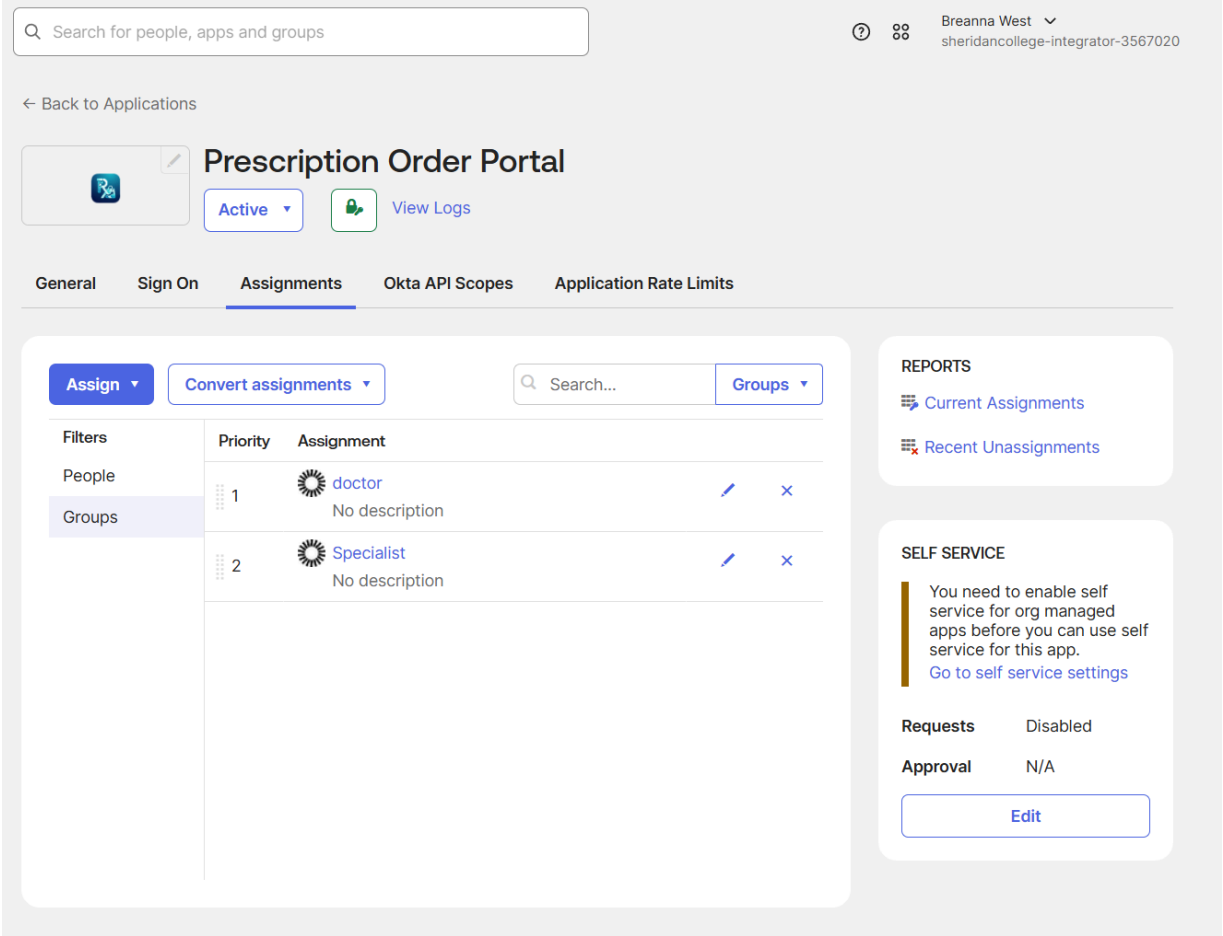
Created groups based on employee roles: Doctor, Nurse, Specialist, Surgeons, Assistants, Administrative Users. Also included a group for admitted patients who may have identities for wifi access.

Patient Data Portal Application



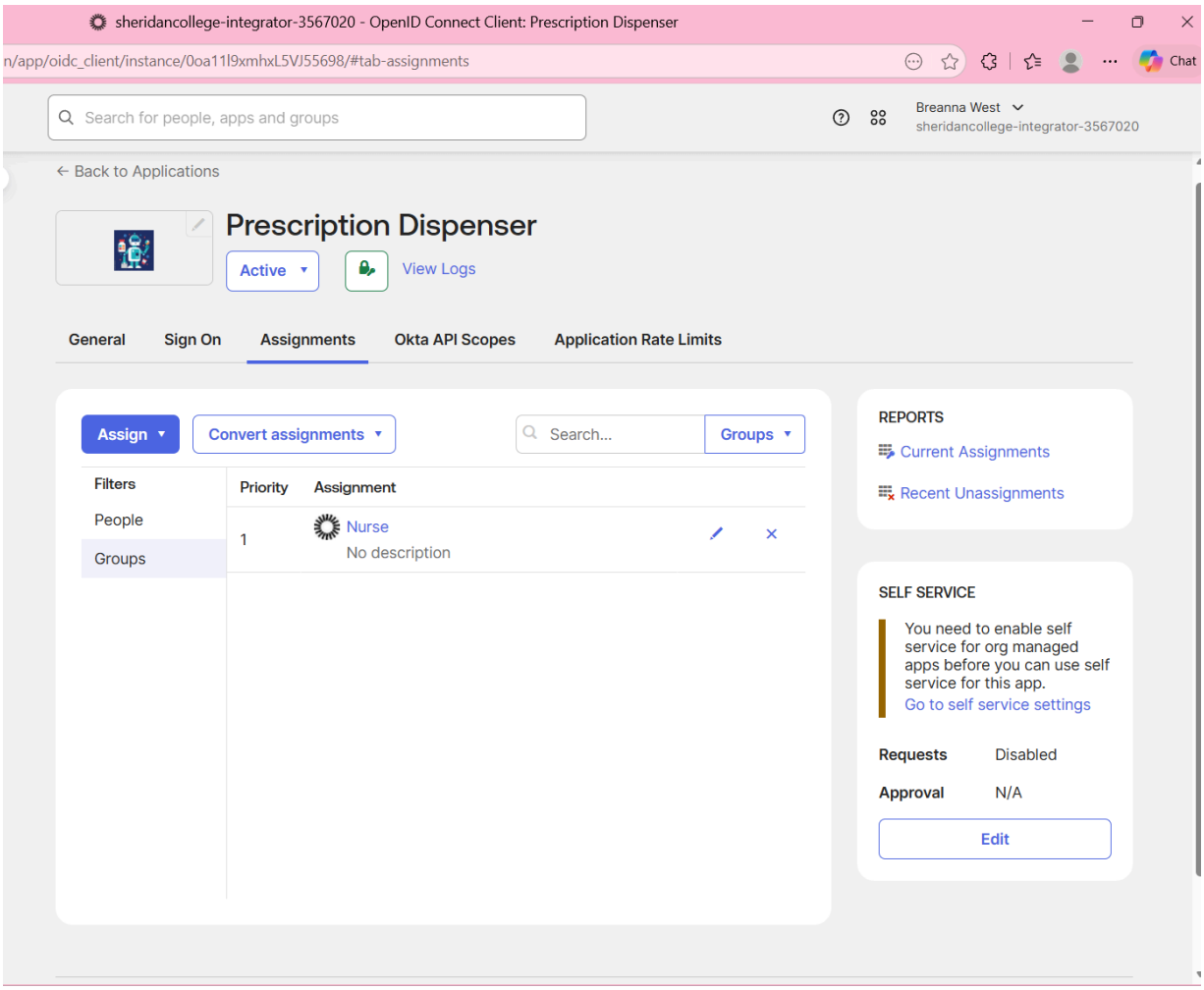
Created the Patient Data Portal application which will store electronic health records of all patients. This application is only accessible by doctors, surgeons and specialists.

Prescription Order Portal Application



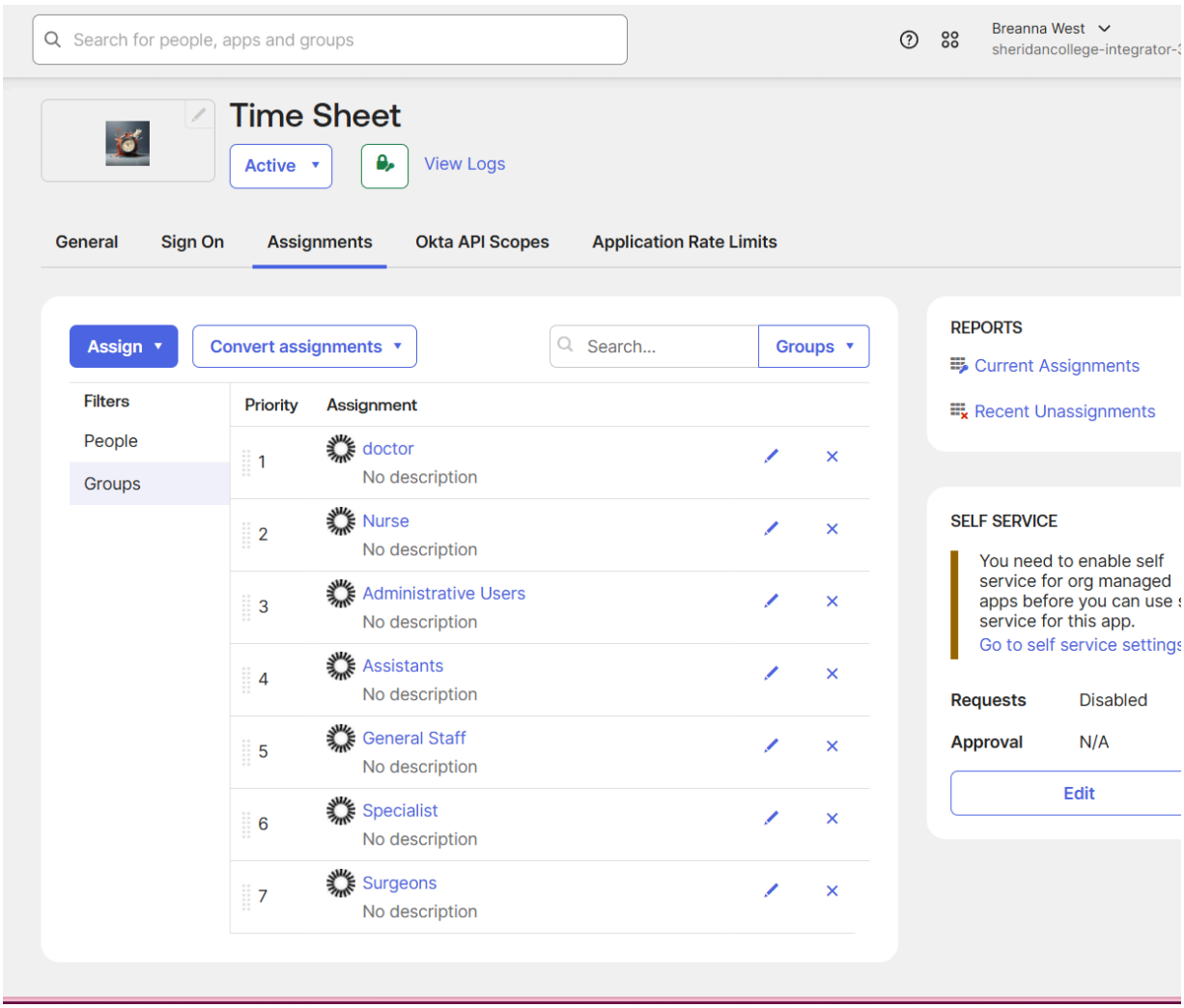
Created a Prescription Order Portal application used to prescribe medications to patients. Access to this application is limited to doctors and specialists but patients still require a nurse to dispense the medication ensuring the separation of duties.

Prescription Dispenser Application



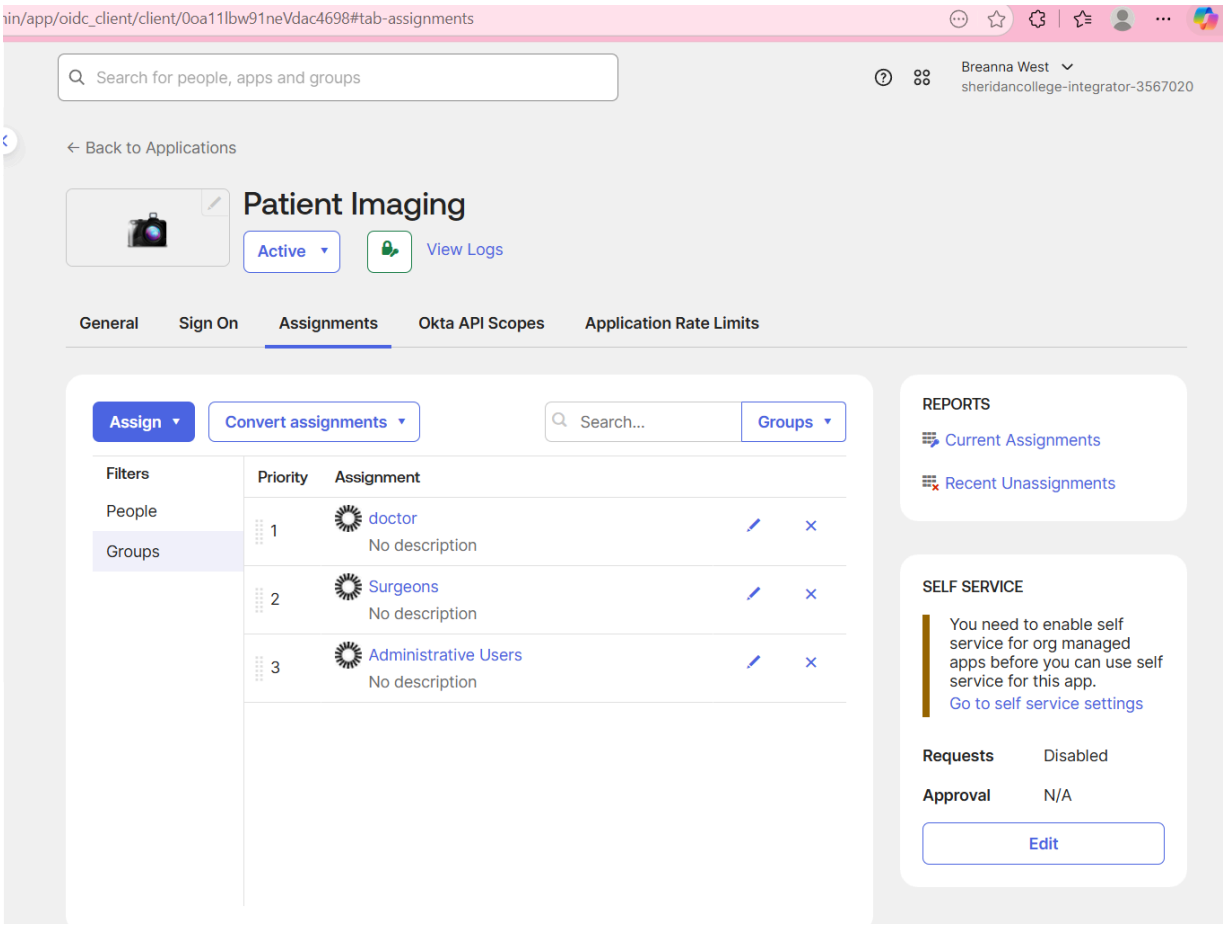
Created a Prescription Dispenser Application to enable nurses to dispense prescriptions for patients. This app is the second part of the 2 step process for obtaining medications for patients. This will ensure no one person can abuse access to narcotics or other drugs.

Time Sheet Application



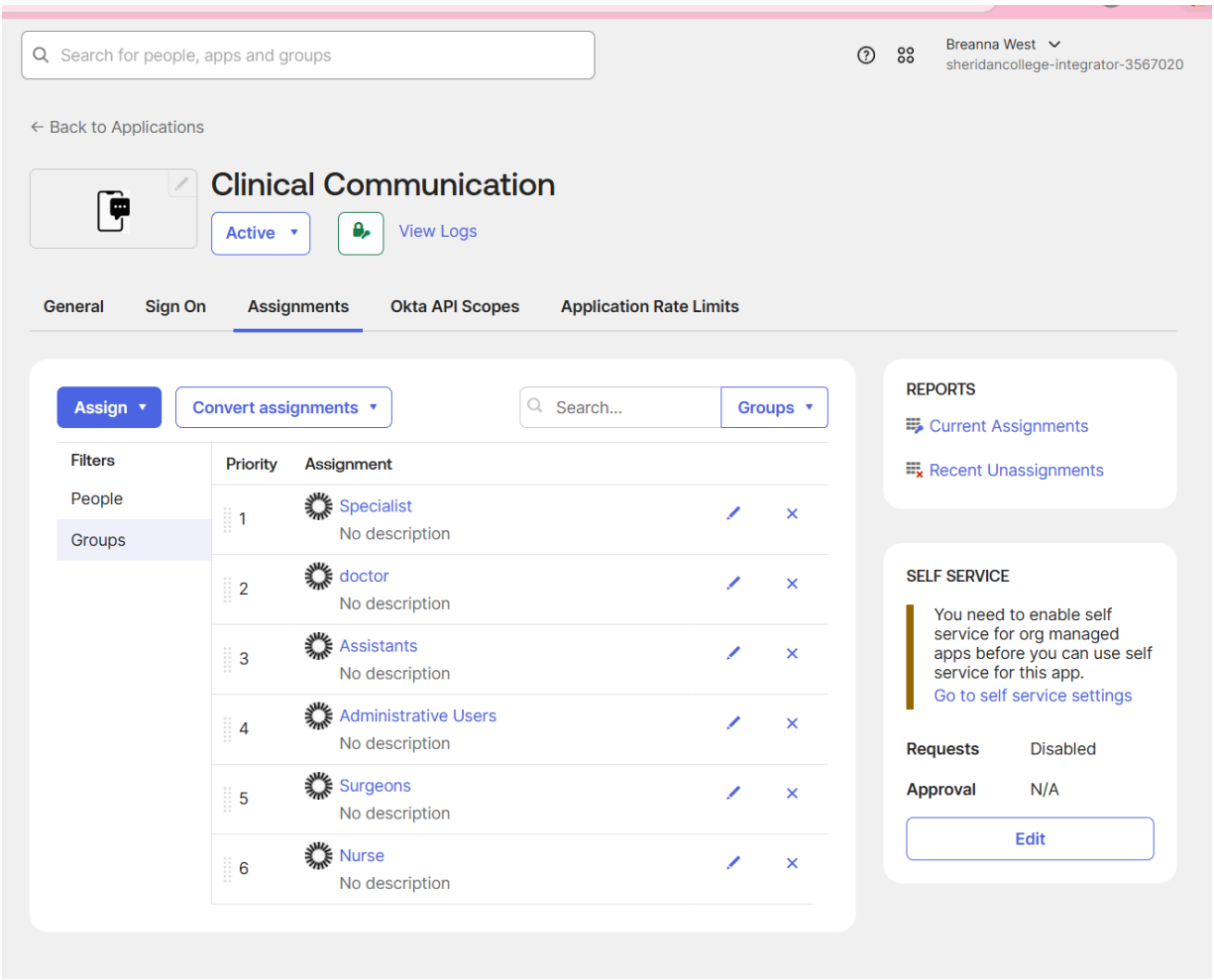
Created the Time Sheet application to allow all employees to view their schedules and punch for their shift times. This app will also allow administrators to handle payroll and employees can track hours worked. The application is accessible to every employee.

Patient Imaging Application



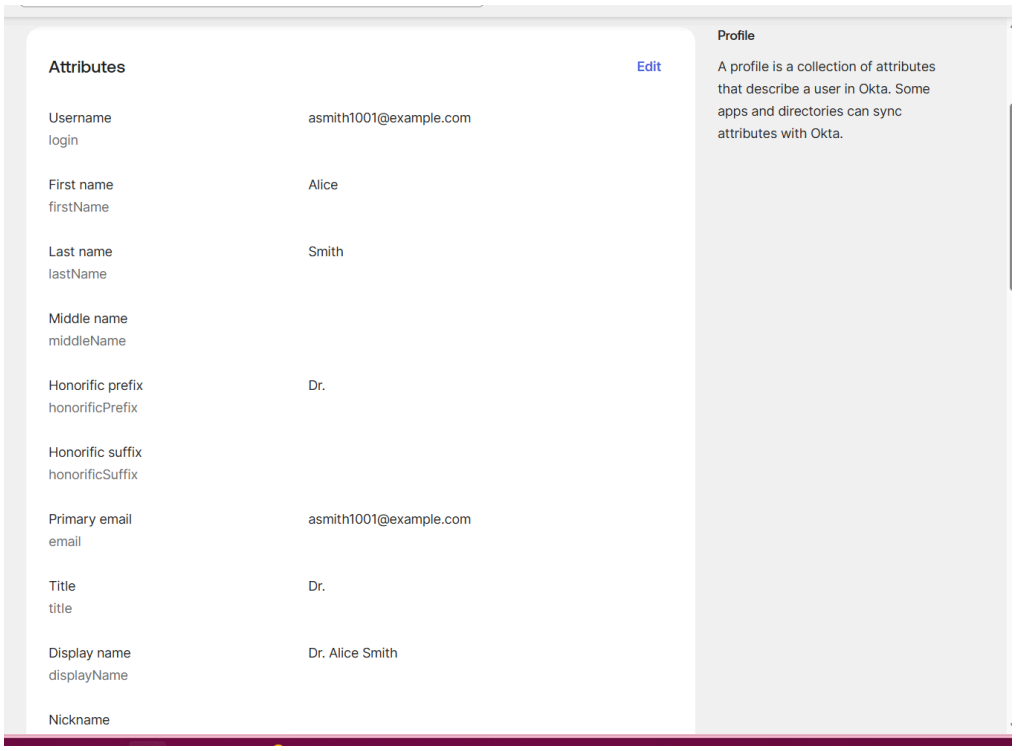
Created a Patient Imaging application to handle sensitive imaging data from MRIs, X-Rays, Ultrasounds, CT Scans and PET scans. This application is only accessible by doctors, surgeons and administrative users.

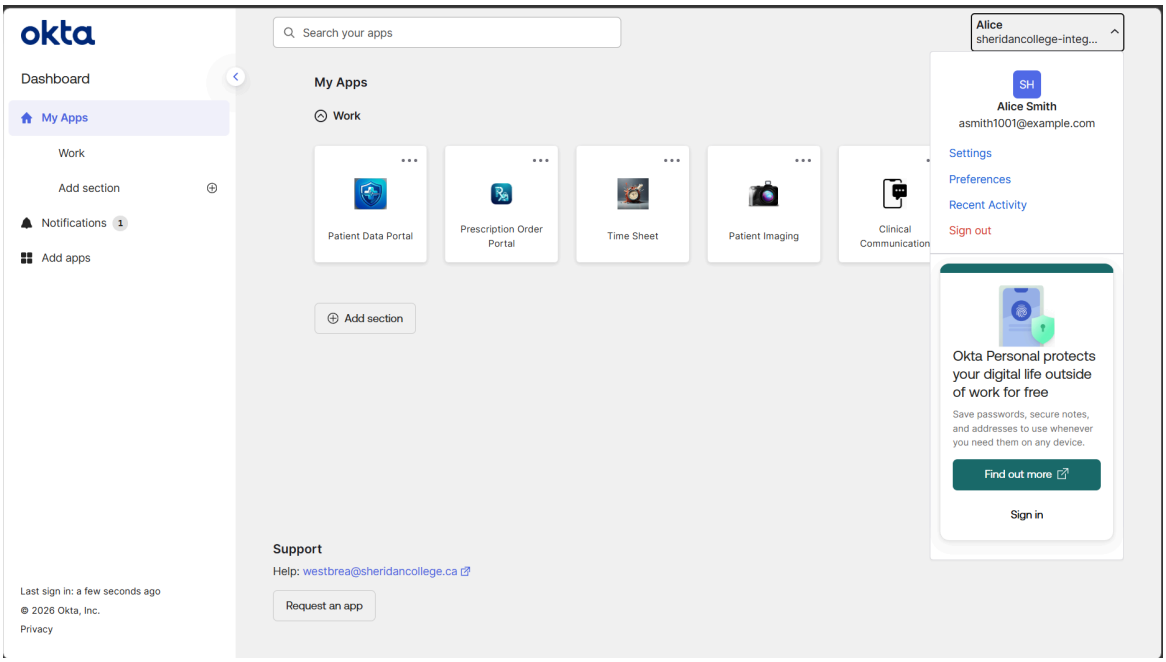
Clinical Communication Application



Created a Clinical Communication application which allows for the employees of the hospital to communicate with each other in a secure and regulatory compliant way. This application is accessible by all hospital employees and helps enforce HIPAA compliance.

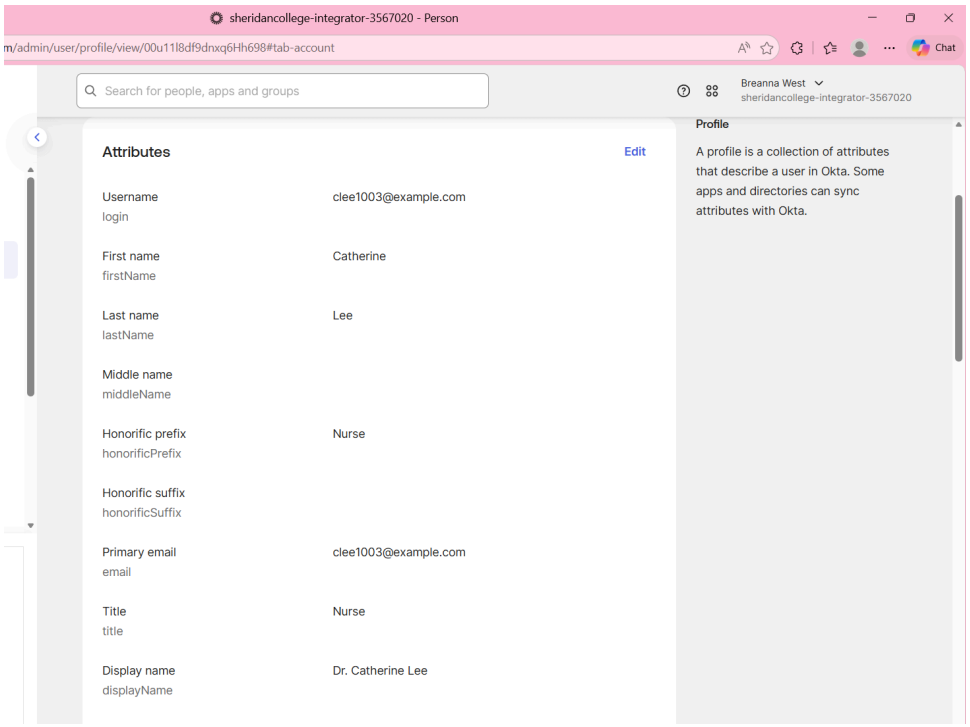
Testing a Doctor Role Account

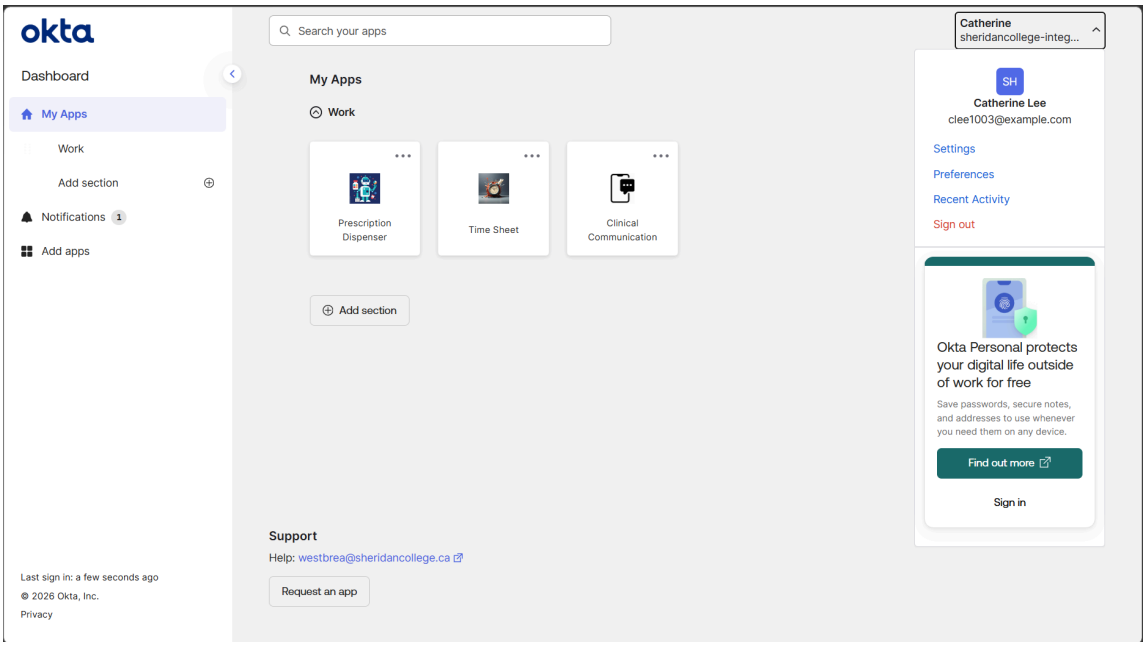




Tested Alice Smith's account who is a Doctor at the hospital, the account could see only the apps applicable to the role (Patient Data Portal, Prescription Order Portal, Time Sheet, Patient Imaging, Clinical Communication).

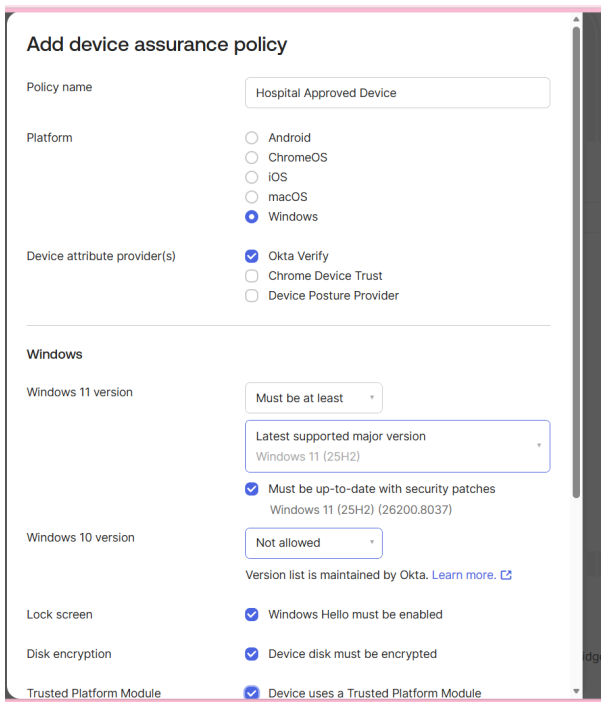
Testing a Nurse Role Account

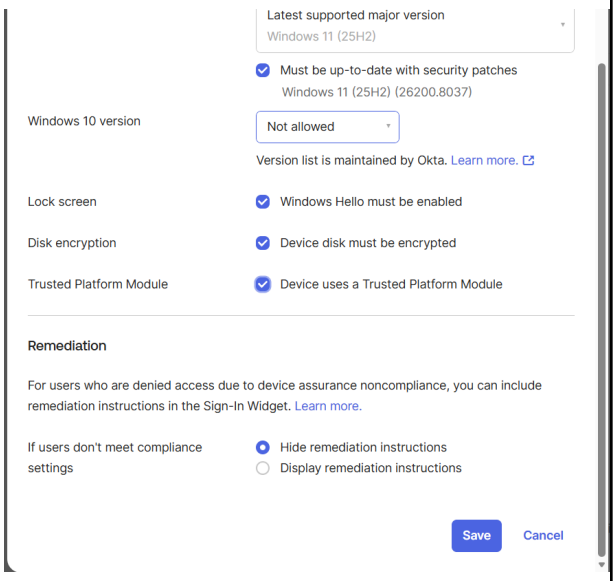




Tested Catherine Lee's account who is a Nurse at the hospital, the account could see only the apps applicable to the role (Prescription Dispenser, Time Sheet, Clinical Communication).

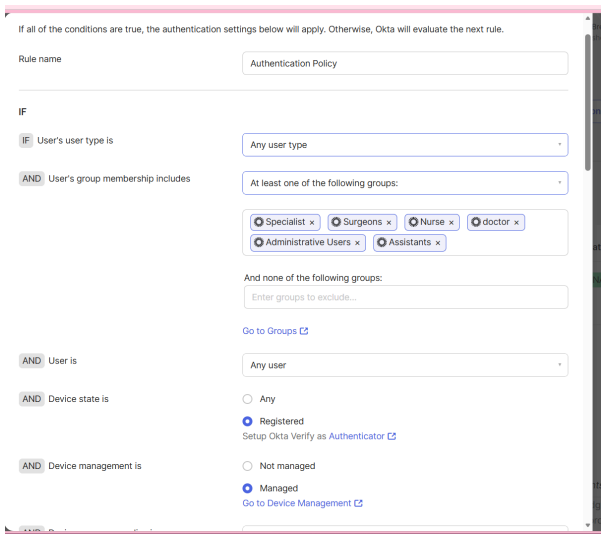
Device Assurance Policy

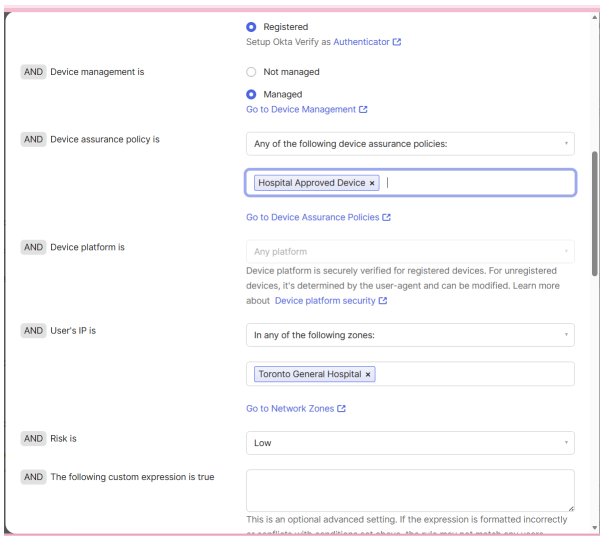


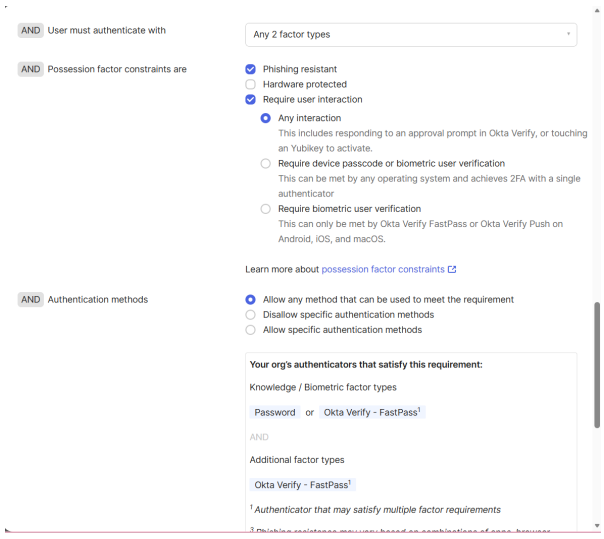


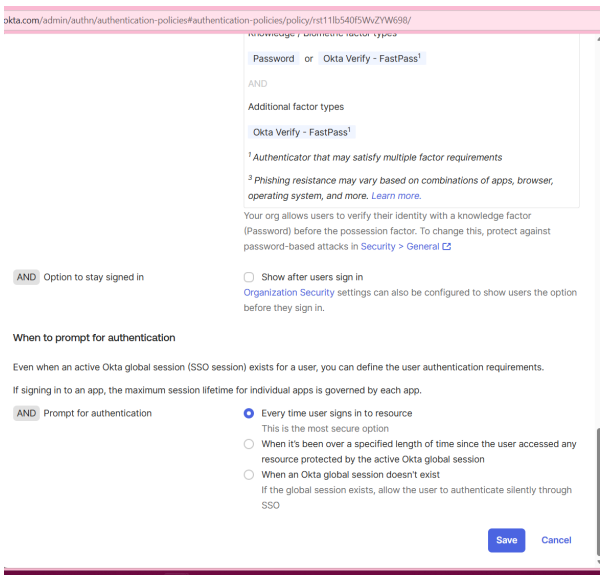
Created a policy to filter out unapproved device configuration before providing successful authentication. The device must be a Windows computer on the latest version of Windows 11 with Window Hello Lock enabled and Disk Encrypted.

Authentication Policy



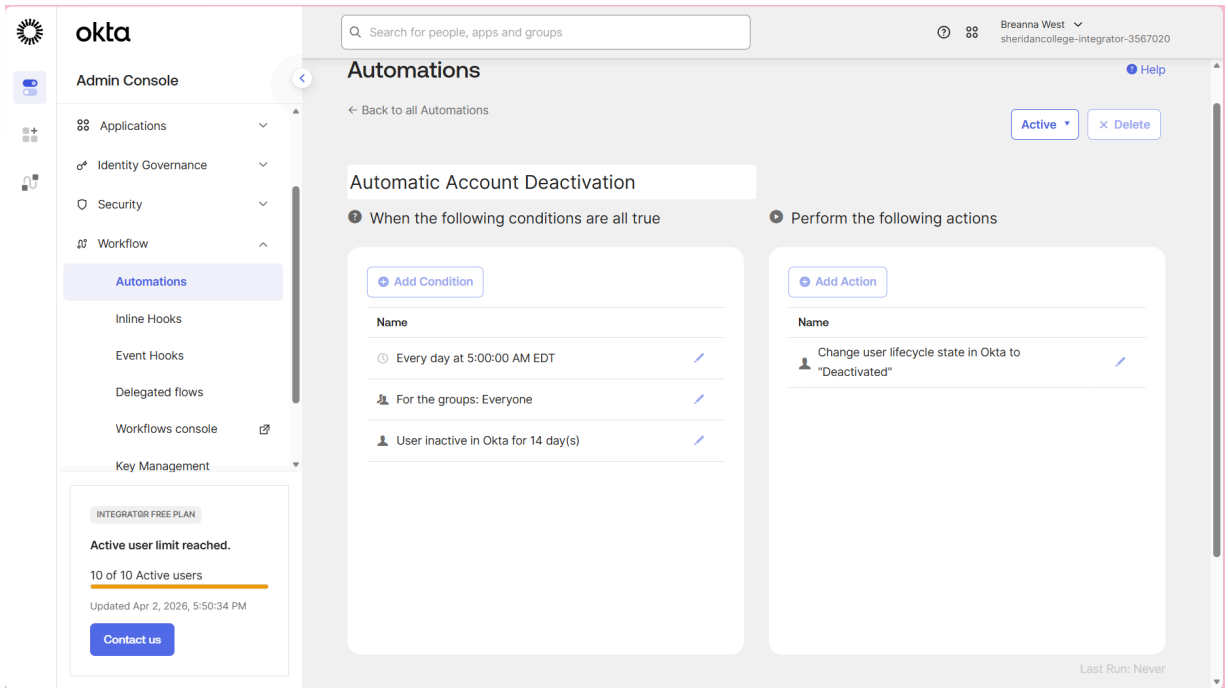






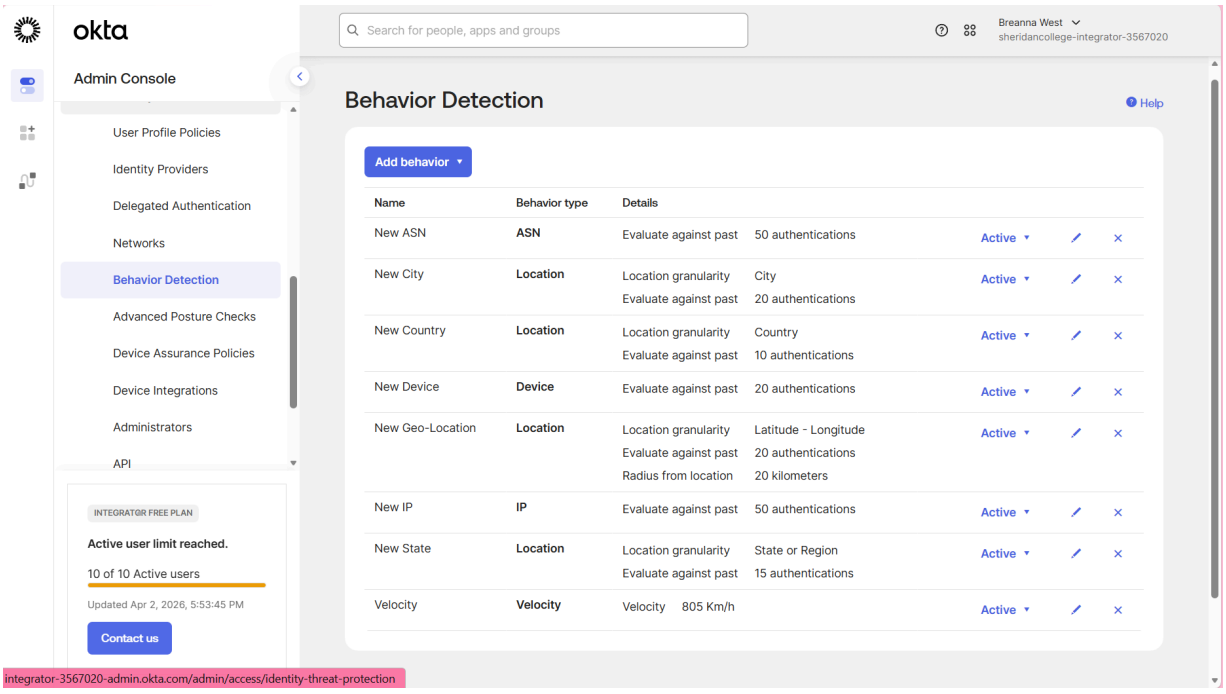
Created a strict authentication policy which applies to all roles. The policy requires the use of a registered and managed device that follows the hospital approved device assurance policy. The device's IP must be within the Toronto General Hospital network. For a successful authentication multifactor authentication via OTP, UbiKey, Password or Okta Verify must be used each time when logging in.

Identity Lifecycle Automation



Created a custom Identity lifecycle automation that will automatically run everyday at 5AM for all active identities. The automation is configured to deactivate an identity if the user has not logged in for more than 14 days. This will limit orphaned account vulnerabilities and will limit the organization's attack surface.

Behaviour Detection Policy



Enforced behaviour detection policies to alert admin for anomalies such as a day shift doctor signing in at night. Detection policies work by comparing actions against the conditions of several previous events. This feature will help to reduce insider threat promoting a zero trust environment.

Results

Implementing this IAM solution has strengthened the hospital's security by ensuring multifactor authentication and adopting a zero trust approach when it comes to each log in request. These ensure that only authorized staff can log in, reducing the risk of credential abuse or unauthorized entry. Compliance checks such as automated monitoring for inactive or orphaned accounts and the use of unique user IDs will keep the hospital aligned with HIPPA requirements and internal policies. By implementing RBAC, ABAC, least-privilege enforcement and separation of duties, employees will only have access to the information and actions necessary for their roles. This reduces the risk of fraud, medication diversion and unauthorized access to patient data.

Analysis

Project Effectiveness

Toronto General Hospital suffered many cybersecurity risks from open access policies, no separation of duties, lack of identity lifecycle management, no role based access control and no attribute based access control. These vulnerabilities ultimately led to the scenario of a laid off nurse using their credentials to leak sensitive data that they should have never had access to. The project proposal to move to a Okta based IAM solution addresses all of the vulnerability concerns and secures the hospital from further threats. The proposal places a large emphasis on role based access control so that employees only have access to what they need to complete their work. This is followed up with attribute based access control to ensure that authentication is done through secure systems. Applications have built in assignments to enforce role based access control. Okta also enabled automatic identity deactivation with the use of automations. Authentication policies are used organization-wide with an emphasis on zero trust, Users must login in on approved devices, on an approved network and must present multiple factors. Overall, the hospital security posture through an Okta IAM solution is strong and effective against the original scenario and future attacks.

Project Limitations

Project limitations mainly centered around the use of the Okta demo environment. The demo restricted our user deployment to ten active users out of the fifty that we attempted to add. This slightly prevented us from being able to do realistic department sizes and shift rotation. Physical access controls such as door reader, badge based authentication and secure physical entry could not be implemented. Okta also does not support discrete mandatory access control, where access is enforced based on classification or labels. Okta’s model is more role-based and group-based, this is not suitable for label based security models. Restrictions such as limiting doctors to only the patients assigned could also not be enforced as it would need to be implemented through an electronic health record system.

Conclusion

Our project with Toronto General successfully demonstrated the proposal and implementation of a functioning IAM workflow using Okta. We managed to implement user lifecycle automation and realistic role based access for doctors, nurses, surgeons, specialists etc. Some major achievements throughout this project were our ability to build a dataset that reflected a healthcare organization. We successfully implemented group based access for different roles and validated lifecycle transitions such as activation and deactivation.

Through this we learned from okta's limitations and strong points. Okta is great at authentication, SSO and authorization but it cannot enforce physical access controls, mandatory access control models and record level restrictions. This provided a greater insight into IAM architecture and the boundaries of some cloud identity platforms. The experience has strengthened our ability to design around platform limitations and think critically about how identity data works in an organization.

References

Access Management- AWS Identity and Access Management (IAM) - AWS. (n.d.). Amazon Web Services, Inc. https://aws.amazon.com/iam/?nc=sn&loc=1&refid=6e78b6f1-dfd8-49b4-ae84-4527ca1881cb

Duo, C. (2026, March 31). *Agentic IAM*. Cisco Duo. https://duo.com/solutions/agentic-ai-security

IAM overview. (n.d.). Google Cloud Documentation. https://docs.cloud.google.com/iam/docs/overview

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2020, December). *NIST SPECIAL PUBLICATION 1800-26A*. Retrieved March 4, 2026, from https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html

Optimal IDM. (2024, May 21). *What are the three types of authentication?* Optimal IdM. https://optimalidm.com/resources/blog/types-of-authentication-methods/

Sande, S. (2025, August 8). Hospital medical hierarchy Every Pre-Med should understand. *MedSmarter Prep*. https://www.medsmarter.com/blog/hospital-hierarchy-every-pre-med-should-understand/

US Department of Health and Human Services. (2024, July 19). *HIPAA for professionals*. Retrieved March 4, 2026, from https://www.hhs.gov/hipaa/for-professionals/index.html

What is Role-Based Access Control (RBAC)? (2024, June 3). Okta. https://www.okta.com/identity-101/what-is-role-based-access-control-rbac/

Mestci, H. (2025, April 8). *RBAC vs ABAC: Main differences and which one you should use*. OSO. Retrieved March 7, 2026, from https://www.osohq.com/learn/rbac-vs-abac

Rawat, A. (2025, December 31). *Identity and Access Management in Healthcare: Core Components, Challenges, and Best Practices*. AppInventiv. Retrieved April 3,

2026, from
https://appinventiv.com/blog/identity-and-access-management-in-healthcare/