Product Requirements Document (PRD)

Access Management Portal (AMP) web application – Aga Khan University Hospital

1. Overview

The Aga Khan University Hospital (AKUH) requires a secure, web-based Access Management Portal (AMP) to digitize user access requests for systems like EHR, PeopleSoft, and PACs. The AMP replaces manual paper-based workflows with a streamlined, auditable, and compliant solution.

2. Goals & Objectives

Primary Goal: Digitize and secure the user access request process at AKUH.

Objectives:
1. Eliminate inefficiencies in paper-based requests.
2. Provide role-based dashboards for requesters, approvers, HR, and ICT admins.
3. Implement secure authentication with MFA.
4. Ensure HIPAA & Data Protection Act compliance.
5. Maintain immutable audit trails with blockchain logging.
6. Enable reporting and analytics for access management.

3. Key Users & Roles

• Requester (Staff): Submit new/additional rights/reactivation/termination requests, track status.

• COS: Submit new/additional rights for physicians, track status.
• Manager/Supervisor: Approve/reject staff requests, view history.
• HR: Request account terminations/reactivations and Approve reactivations / terminations, ensure compliance.
• ICT Admin: Fulfill approved requests, manage users/roles, view audit logs, generate reports.

4. Features & Requirements

4.1 Authentication & Security

• MFA (OTP via SMS/Email/Authenticator App) after login.
• Passwords stored with bcrypt hashing.
• JWT for session management.

• Role-Based Access Control (RBAC).
• SSL/TLS encryption in transit and PostgreSQL pgcrypto for encryption at rest.
• Blockchain-based immutable logging for compliance.

4.2 Core Modules

A. Login & MFA
- Secure login (username + password).
- OTP screen for secondary authentication.
- Password reset with strength validation.

B. User Management
- Create, update, deactivate users.
- Assign roles and departments.
- Search & filter users.
- Track login history.

C. Access Requests
- Submit new access / additional rights / reactivation / termination requests.
- Dynamic form based on request type. Fields are Payroll, First and last name, email, and username and Template name

-For COS; Dynamic form based on request type. Fields are Payroll, First and last name, email, username, Template name, provider group, provider type, specialty, service, admitting (Yes/No), Ordering Physician (Yes/No), Sign (Orders, Reports, Both, Neither) and Co-sign (Orders, Reports, Both, Neither)
- Attach supporting documents if needed.
- Track request lifecycle.

D. Dashboards
- Requester: Request history, status tracker.
- Manager: Pending approvals, approve/reject with comments.

- COS: Request history, status tracker.
- HR/COS: Focused on reactivations/terminations.
- ICT Admin: Fulfillment queue, completion marking, reports, audit logs.
- Admin (Analytics): KPIs, request volumes, approval timelines, system usage.

E. Audit Logs
- Tamper-proof log of all actions.
- Filters by user, action type, date range.
- Export to CSV/PDF.

F. Reports & Analytics
- Generate reports on requests, processing times, and compliance.

- Visual charts: pie, bar, line (requests by type, department, status).
- Downloadable summaries for auditors.

5. API Endpoints

Auth & Security:
- POST /api/auth/login
- POST /api/auth/verify-otp
- POST /api/auth/reset-password
- PUT /api/auth/update-password

User Management:
- GET /api/users
- GET /api/users/:id
- POST /api/users
- PUT /api/users/:id
- DELETE /api/users/:id

Requests:
- GET /api/requests
- GET /api/requests/:id
- POST /api/requests
- PUT /api/requests/:id
- DELETE /api/requests/:id

Audit Logs:
- GET /api/audit-logs

Dashboards:
- GET /api/dashboard/admin
- GET /api/dashboard/ict

6. System Architecture

• Frontend: HTML, CSS, JavaScript (Bootstrap, React optional).
• Backend: PHP + Node.js (for real-time notifications).
• Database: PostgreSQL with indexed queries.
• Security: Blockchain logging, JWT, MFA.
• Hosting: AWS EC2 (App), AWS RDS (PostgreSQL), GitHub Actions CI/CD.

7. Database (Core Tables)

• Users: user_id, name, email, phone, role_id.
• Roles: role_id, role_name, permissions.
• AccessRequests: request_id, requester_id, system_id, type, status, dates.
• AuditLogs: log_id, user_id, action, timestamp, details.
• Systems: system_id, system_name, description.

8. UI/UX Guidelines

• Consistent teal/green + white color scheme.
• Role-based navigation in sidebar.
• Clean typography & responsive design.
• Accessibility (WCAG-compliant).
• Consistent layout across Login, MFA, Dashboards, and Reports.

9. Constraints

• Must comply with HIPAA and Kenya's Data Protection Act.
• Resource limits (budget, staff adoption).
• Integration scope limited (Phase 1 excludes full HR onboarding).

10. Success Metrics

• 60%+ reduction in audit preparation time.
• Requests processed in minutes, not days.
• Zero security breaches / audit non-compliance.
• Positive adoption feedback from staff.

11. Future Enhancements

• Integration with HR systems for automated onboarding/offboarding.
• Mobile app for request approvals.
• Advanced analytics for trend monitoring.
• Multi-tenant expansion across Aga Khan Health Network.

12. Role Mapping & Templates

• Users will be mapped to role-based templates that determine whether they are Requesters, Approvers, HR, ICT Admin, or Auditors.
• Templates define the actions and dashboards available to the user.
• Admins can assign one or more templates to a single user (e.g., a user can be both Manager and ICT Admin).
• Depending on the template assigned, users will have access to specific dashboards,

metrics, and reports.
• Requester Templates:
  - Can request: New Access, Additional Access, Account Reactivation (requires HR approval).
• HR Templates:
  - Can approve Reactivation requests.
  - Can also initiate Account Deactivation requests.
• Manager Templates:
  - Can approve/reject team requests and provide comments.
• ICT Admin Templates:
  - Can view all approved requests, fulfill them, mark completion, and manage user accounts.
  - Can generate reports and review audit logs.
• Auditor Templates:
  - Can only view immutable audit logs and compliance reports.
• Users can view specific metrics, dashboards, and KPIs depending on the template(s) assigned to them.

13. Forgot Password & OTP Flow

• Users who select 'Forgot Password' will be required to enter their registered email/username.
• An OTP will be sent via SMS or email.
• User must verify the OTP before setting a new password.
• New password must comply with hospital security policy (length, complexity, special characters).