Official IAM Procedure for Brussels CHR Hospital

Purpose

To establish secure, auditable, and compliant Identity and Access Management (IAM) controls for key hospital workflows managing patient admission, surgery planning, medication prescription, and appointment scheduling.

Scope

Applicable to all users accessing hospital systems including OASIS+, QBLOC, DXPLANNING, and related e-health platforms, encompassing reception staff, medical secretaries, doctors, anesthetists, pharmacists, and nursing staff.

Responsibilities

- **All users**: Authenticate according to procedure before accessing patient or scheduling data. Use systems within authorized role scopes.
- **IAM administrators:** Maintain authentication infrastructure, enforce MFA, SSO (OAuth 2.0 + OIDC), and role-based access (RBAC, ABAC).
- **Process owners:** Ensure compliance with procedure and update as needed.
- **Compliance officers:** Audit access logs and review SoD policies.

Procedure

1. Authentication and Access Control
   - Users authenticate securely using MFA (badge + PIN or OAuth-based SSO via Okta).
   - Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) restrict system functionalities per user role and context.
   - All login events and critical operations are logged for auditability.
2. Appointment Scheduling (DXPLANNING)
   - Medical secretaries authenticate with MFA and SSO.
   - Patient searched or temporary profile created.
   - Appointment types selected, and available time slots proposed by DXPLANNING.
   - Confirmed appointment logged and added to doctor’s schedule.
3. Patient Admission (OASIS+)
   - Receptionists authenticate with MFA and open OASIS+.
   - Patient identity verified and/or created with integration to national registry validation.
   - Insurance coverage is verified, and admission is confirmed only if coverage is validated.
   - All actions are securely logged.

4. Surgery Planning (QBLOC)

    - Surgeons and anesthetists authenticate with MFA and SSO.
    - Surgery requests initiated with patient verification via OASIS+.
    - Operating room slots and anesthetists allocated with logged approvals.
    - Notifications sent automatically and surgery schedule is finalized with audit trail.

5. Medication Prescription (OASIS+)

    - Doctors authenticate with MFA and insert patient ID card for verification.
    - Therapeutic link confirmed or created via e-Health portal.
    - Prescriptions recorded digitally within OASIS+ prescription module with logging.
    - Secure completion and patient ID card returned.

6. Audit and Monitoring

    - All system events related to authentication, access, and critical actions are logged.
    - Periodic reviews of access rights and SoD implemented to ensure compliance.

7. Incident Management and Training

    - Incidents involving access breaches or suspicious activity reported per hospital policy.
    - Ongoing training delivered to all users on secure access management and responsibilities.

8. Review and Update

    - Procedure reviewed annually or following significant process/system changes to remain effective and compliant.