Access Policies

Abstraction:

The access policies for our proposed healthcare system involves defining who can access what information and what actions they can perform within the system. This will establish some fundamental access control rules that align with SOC 2 security and compliance standards. These rules will be broad to cater to various healthcare systems, and specific implementations may adjust according to local regulations and policies.

General Principles:

- **Least Privilege:** Users should only have access to the information and resources that are necessary for their job functions.
- **Patient Privacy:** Patients' health information must be protected, ensuring it is accessible only to those directly involved in their care or those granted explicit permission by the patient.
- **Audit Trails:** Access and actions within the system should be logged to enable accountability and facilitate audits.

Access Control Policies

Doctors:

- **Access to Appointments:** Doctors can access appointment details for their patients only.
- **Access to Medical Records:** Doctors can view and update medical records for their patients. They can also view their own scheduled appointments and details about those appointments.
- **Prescription Privileges:** Doctors can create, update, and view prescriptions for their patients.
- **Contact Information Access:** Doctors can view their own profile and contact information but cannot access personal information of other doctors beyond what is necessary for patient care coordination.

Patients:

- **Access to Own Records:** Patients can view their own medical records, including diagnoses, treatments, prescriptions, and appointment history.
- **Appointment Management:** Patients can view and manage their own appointments.
- **Privacy Controls:** Patients have the right to request restrictions on certain uses and disclosures of their health information.

Administrative Staff:

- **Appointment Management:** Administrative staff can create, update, and view appointments for all doctors and patients.
- **Patient Management:** Can view and update patient profiles to maintain current and accurate information.
- **Doctor Profiles Access:** Can manage doctor profiles, including scheduling and contact information.

IT and System Administrators:

- **Technical Access:** Have access to the system for maintenance and updates but are restricted from accessing patient health information unless necessary for system functionality and integrity.
- **Security Management:** Responsible for managing user accounts, including doctors' login credentials, ensuring secure password policies, and managing access rights.

Implementation Notes

- Implement role-based access control (RBAC) within the system to enforce these policies effectively.
- Use views, stored procedures, and triggers in the database to enforce access control measures at the data layer.
- Encryption and secure communication protocols should be used to protect data in transit and at rest, especially for sensitive information like passwords and health records.
- Regular audits and reviews of access logs should be performed to ensure compliance with the access control policies and to detect any unauthorized access attempts.