Security Features for the Hospital Management System (HMS)

The following are seven essential security features along with brief descriptions:

1. **User Authentication:**
    - Verify the identity of users attempting to access the system. This involves user ids and passwords. It ensures that only authorized individuals can enter the system and once authenticated, users can only access and manage information relevant to their own accounts and roles within the Hospital Management System.
2. **Role-Based Access Control (RBAC)**
    - Restricts system access based on the user's role. Different roles such as Doctor, Nurse, Receptionist, Lab Technician, and Patient have varying levels of access to data and functionalities. For example, a Doctor can view patient appointments and prescriptions, while a Receptionist can manage admissions and invoices. This ensures that sensitive data is only accessible to authorized personnel.
3. **Data Encryption**
    - Sensitive data like patient records, personal information, and medical history are encrypted both at rest and in transit. This prevents unauthorized access and data breaches, even if the database or communication channels are compromised.
4. **Input Validation and SQL Injection Prevention**
    - Ensures that user inputs are valid and safe. All input fields (e.g., patient registration, appointment scheduling) are validated to prevent SQL injection and cross-site scripting attacks. Parameterized queries and prepared statements are used to safeguard against malicious data entry.
5. **Password Management:**
    - Securely stores and handles user passwords. This includes hashing passwords (not storing them in plain text) and enforcing password complexity rules.

6. **Audit Logs and Monitoring**
    - Records user activities and system events. This includes tracking changes to patient records, admission details, invoice generations etc. to identify suspicious activities. This helps in tracking who accessed what data and when, which is essential for accountability, detecting suspicious behavior, and forensic analysis in case of a security breach.
7. **Session Management and Timeout**
    - User sessions should be managed securely, with session timeouts implemented after a period of inactivity. This minimizes the risk of unauthorized access if a user leaves their session active on a shared or public device. This involves creating a unique session ID upon login, securely storing it, and invalidating it upon logout or after a period of inactivity.

==========