تصميم إطار أمني لنظام إدارة المستشفيات (HMS) مع التركيز على التحكم في الوصول بناءً على الأدوار (RBAC)

يتضمن تحديد الأدوار، تخصيص الأذونات، وضمان خصوصية البيانات وسلامة النظام. فيما يلي نهج منظم:

1. تحديد الأدوار

تحديد جميع الأدوار داخل نظام المستشفى والمسؤوليات المرتبطة بها. ومن الأدوار الشائعة:

المسؤول (Administrator): إدارة النظام، تخصيص الأدوار، وضبط الإعدادات.

الطبيب (Doctor): الوصول إلى السجلات الطبية للمرضى، سجل الوصفات الطبية، ونتائج التشخيص.

الممرضة (Nurse): الوصول المحدود إلى خطط الرعاية وسجلات صرف الأدوية.

موظف الاستقبال (Receptionist): التعامل مع تسجيل المرضى، المواعيد، ومعلومات الفواتير.

الصيدلي (Pharmacist): عرض الوصفات الطبية وصرف الأدوية.

فني المختبر (Lab Technician): عرض طلبات الفحوصات وتحميل النتائج.

المريض (Patient): الوصول إلى سجلاتهم الشخصية، الوصفات الطبية، ومعلومات الفواتير.

2. سياسات التحكم في الوصول:

وضع قواعد واضحة حول من يمكنه الوصول إلى البيانات بناءً على دوره:

مبدأ أقل الامتيازات: يجب أن يكون لدى المستخدمين الحد الأدنى من الوصول المطلوب لأداء دورهم.

فصل المهام: ضمان عدم حصول أي دور على سيطرة مفرطة (مثل الفصل بين الأدوار التي تدير الشؤون المالية وتلك التي تصل إلى السجلات الحساسة للمرضى).

3. مستويات الوصول إلى البيانات

تصنيف البيانات والوظائف بناءً على الحساسية:

بيانات عامة: معلومات المستشفى، ساعات العمل، وما إلى ذلك.

بيانات سرية: سجلات المرضى، التاريخ الطبي، معلومات الفواتير.

بيانات شديدة الحساسية: تفاصيل التشخيص، الوصفات الطبية، ونتائج المختبر.

تحديد الأذونات (عرض، تعديل، حذف، تحديث) لكل مستوى بناءً على الأدوار.

4.تشفير البيانات

أثناء التخزين: تشفير البيانات الحساسة المخزنة في قاعدة البيانات.

5.تصميم واجهة المستخدم

تقييد عناصر واجهة المستخدم بناءً على الأدوار (مثل منع الأطباء من الوصول إلى واجهة الفواتير).

توفير رسائل واضحة عند رفض الوصول.

6.مراجعة الأدوار الدورية

تعطيل الحسابات للمستخدمين الذين لم يعودوا مرتبطين بالمستشفى (مثل الموظفين السابقين).