Privacy in Healthcare

Yichun Zhou

Privacy in Healthcare or medical privacy is to keep the security and confidentiality of patient records. Modern concerns include the level of disclosure to insurance companies, different workers, and other third parties. Also, more health records are stored electronically, that have raised new concerns about privacy.

Many countries, including Australia, Canada, and the United States have enacted laws that try to protect people's medical privacy. The United States has passed the Health Insurance Portability and Accountability Act (HIPAA) to increase privacy precautions within hospitals and other medical-related facilities.

**HIPAA**

HIPAA (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information. The act contains five sections or titles, which can be summarized and broken up into two main rules, the Privacy Rule and the Security Rule.

* The Privacy Rule protects healthcare records and other personal health information (PHI) based on national standards. This applies to covered entities such as health plans and healthcare providers that conduct transactions electronically.
* The Security Rule guards patients’ electronic medical records which are created, received, used or maintained by a covered entity by establishing national standards.

The main purposes of HIPAA it to renovate the flow of healthcare information, regulate how Personally Identifiable Information maintained by the medical and healthcare insurance institutions should be protected from theft and fraud, and issue limitations on healthcare insurance coverage.

**HITECH Act**

The HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 is created to increase the use of electronic health records (EHR) and the accessorial technology in the United States.

The HITECH Act contains four subtitles:

* Subtitle A: Promotion of Health Information Technology
* Subtitle B: Testing of Health Information Technology
* Subtitle C: Grants and Loans Funding
* Subtitle D: Privacy (closely related to HIPAA)

HITECH Act is very important and it has changed health IT. One of the primary influences of the HITECH Act is that the EHR adoption rate for qualified hospitals increased from 3.2% to 14.2% in eight years, from 2008 to 2015.

**HITECH Act vs. HIPAA**

HITECH and HIPAA, are independent laws, but they do augment each other in certain ways. For example, HITECH specifies that technologies and technology standards created under HITECH will not compromise HIPAA privacy and security laws. HITECH also requires that any physician or hospital that attests to meaningful use must have performed a HIPAA security risk assessment.

**EHR**

An electronic health record (EHR) is an electronic copy of a patient’s paper chart and a real-time, patient-centered record that makes information available instantly and securely. Also, an individual's official health document that is shared among multiple facilities and agencies (authorized users).

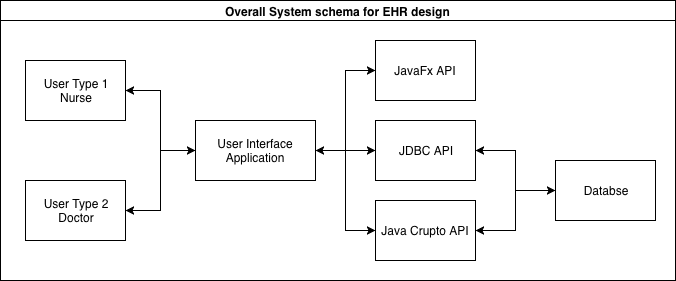
EHRs usually contain patients’ medical data, including visit history, diagnoses, medications, treatment plans, immunization dates, allergies, radiology images, and laboratory and test results. Also, EHRs allow access to evidence-based tools that providers can use to make decisions about a patient’s care and can help to automate and streamline providers’ workflow.

EHRs can ensure medical privacy in certain ways. EHRs in the U.S. must be HIPAA compliant. The HITECH Act also grants regulations meant to assure the safety of EHRs. Still, HIPAA and the HITECH Act are just the baselines for EHR protection. EHRs should also have other safety features developed into the platform such as an audit trail system, state-of-the-art data centers, access control tools, encryption and more.

As of late 2017, the clinic EHR market is mainly a battleground between two firms: Epic Systems Corporation and Cerner Corporation. Other top EHR vendors include Allscripts, Meditech, AthenaHealth and eClinicalWorks.

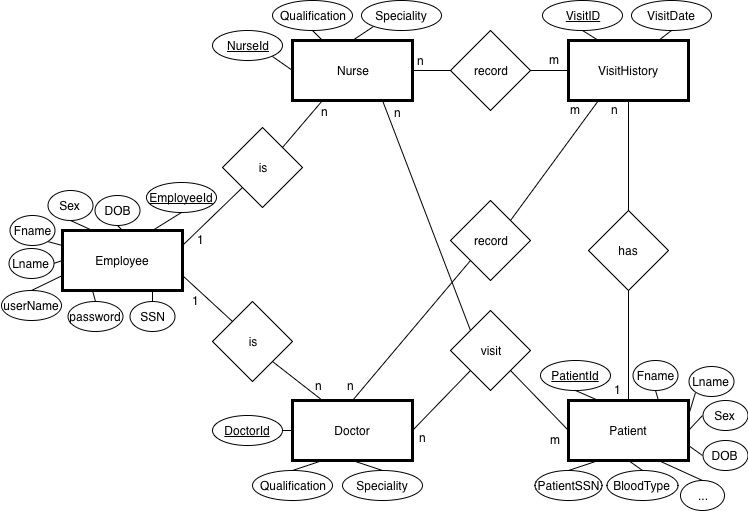
**EHR Example**

Below is an example of the system and database design for an EHR program.



*Fig.1 Overall system schema for an EHR design*

Fig.1 is the overall system schema for an EHR design. There is a total of five fundamental parts in the example schema: The User interface provides a GUI user application with two types of users, a doctor or a nurse. The JDBC API offers database connection functions, while JavaFX API supports the GUI, and Java Crypto API is able to encryption data. The last component is the database that lies at the bottom of the abstraction hierarchy to store patient data records, as well as encrypted content.

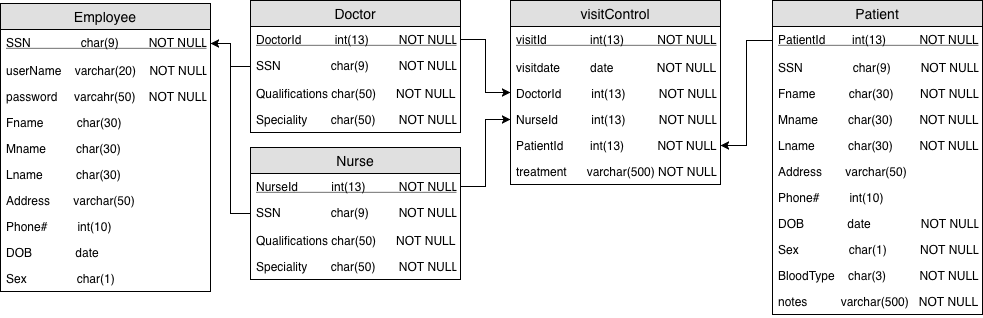


Overall ER Diagram for EHR System

1:n relationship between Employee and Doctor and Employee and Nurse as a there could be many doctors as employees, and one doctor can only register once as an employee. The same relationship between Employee and Nurse entities.

1:n relationship between Patient and VisitHistory, a patient can have many visit histories, but one visit history cannot belong to multiple patients.

The rest n:m relationship is relatively simple, such as patients can visit multiple doctors are nurses, and doctors or nurses can record several visit histories.



Relational Database Schema

Primary Key (PK)

SSN is the PK in Employee table, as it uniquely identifies each employee.

DoctorID is the PK in Doctor table, as it uniquely identifies each doctor.

NurseID is the PK in Nurse table, as it uniquely identifies each nurse.

PatientID is the PK in Patient table, as it uniquely identifies each patient.

VisitID is the PK in VisitControl table, as it uniquely identifies each visit history.

Foreign Key (FK)

DoctorID is FK in VisitControl table references to DoctorID in Doctor table.

NurseID is FK in VisitControl table references to NurseID in Nurse table.

PatientID is FK in VisitControl table references to PatientID in Patient table.

SSN is FK in Doctor table references to SSN in Employee table.

SSN is FK in Nurse table references to SSN in Employee table.

References

<https://en.wikipedia.org/wiki/Medical_privacy>

<https://searchhealthit.techtarget.com/definition/HIPAA>

<https://searchhealthit.techtarget.com/definition/HITECH-Act>

<https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act>

<https://en.wikipedia.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act>

<https://www.sciencedirect.com/science/article/pii/S1877050915025764>

<https://www.healthit.gov/faq/what-electronic-health-record-ehr>

<https://www.academia.edu/27145315/DESIGN_AND_IMPLEMENTATION_OF_PATIENT_MANAGEMENT_SYSTEM>

<https://searchhealthit.techtarget.com/definition/electronic-health-record-EHR>