The healthcare sector has adopted information technology to expedite the process of treatment and simplify business operations. Electronic healthcare records (EHR) are widely used and shared by healthcare professionals. In many cases, patients do not travel to hospitals on a regular basis to meet their doctors or physicians rather they are sending their health status over the Internet via mobile or web apps, and sometimes providing access to their data for care delivery organizations (CDOs).

EHRs contain sensitive information about patients and many security issues apply, including secure collection and storage of EHRs from remote sites, how to provide secure access control to various parties, key management among different CDOs, cyber attacks of healthcare systems, collection and storage of EHR (e.g. multiple CDO). In such scenarios, how the data is securely shared among different parties and how the access control policies are defined. All these problems are visible when one has understood various processes.

As you see that roles of people define their privileges to access information science for some practical purpose. For an instance, a doctor should have access to the complete EHR of a patient, a medical researcher should have access to patient medical data without knowing the identity of a patient. A pharmacy personnel or food staff is allowed to access the pharmacy data, which should not be disclosed. It is obvious that patient thinking of is the application of mobile and web apps, which help patients to send their EHR over the network to their healthcare providers.

The technology makes us understand the need of Health Information Technology (HIT), variety of tools and machineries used to expedite the medical treatment process. We have divided the system into different domains: Remote, Data center, CDO and Security Operations Center (SOC). And all domains are interconnected via some ways of information technology. The question at this point is: is this interconnection cyber safe? Have these systems implement proper security measures in their internal processes that make overall system secure?

The problem of security lies in such technologies since we need to ensure that data stored and communicated via these wireless devices and communication channels are secure. It is obvious that physical access to certain mobile devices could compromises all data stored on it. We have to design the placement of data with such an understanding so that remote collection, storage or transmission of data can be secured.

Secure Policies using Guiding Principles

People are actors who have specific roles in healthcare settings. The actors are: Patients, Doctors, Physicians and Nurses etc. The responsibilities of actors are assigned on the basis of their roles in the system.

We have to understand the roles of different people involved in healthcare settings. Once we have understood their roles, we can figure out which data they require while doing their job, e.g.

- A doctor should have access to the complete EHR of a patient, a medical researcher should have access to patient medical data without knowing the identity of a patient.
- Pharmacy personnel or food staff is allowed to access the pharmacy data, which should not be disclosed.
- What privileges should be given in case of emergency.

As you see that roles of people define their privileges to access data in the system, we can group people on the basis of their roles and assign access control policies.

Conclusion

Secure Healthcare Architecture: People, Process and Technology

Yatin Wadhawan, Dr. Clifford Neuman

Information Science Institute, University of Southern California Los Angeles, CA