Electronic Health Records (EHR)

Name

Institution

**Electronic Health Record**

The Electronic Health Record (ERH) is referred to as an electronic communication tool that assists coordination of services, regulatory process, accreditation, education, legal protection, research, efficacy of care, evaluation of the quality, coordination of services, and clinical decision making(Tnmed, 2012). It is the record of normal course of healthcare activities documented electronically.

Documentation is the basis for clinical decision making hence it must be authenticated before and after documentation. In the past, the medical record was documented manually and is immensely limited in terms of availability and accessibility with respect to time (Tnmed, 2012). First, this record was updated manually which used to take one to six months or more in some instances. Moreover, the record took deliberate painstaking efforts to be retrieved.

To ease the documentation and accessibility of information, documentation is scanned manually into an electronic device instantly and is completed as far as the patient leaves hospital. Records when entered electronically require appropriate regulatory requirements and accrediting. It is highly interactive in nature and has multifaceted users i.e., reviewers, patients and stakeholders. Government takes active participation in the maintenance of records because it is an important element in healthcare management (AHIMA, 2012).

The electronic healthcare record is advantageous in a sense that it may have many viewers at the same time and encapsulates a bulk of information technology tools. These record not only assist the healthcare professionals but also patients to maintain their personal health record (PHR) in which their diagnosis, medication, prognosis and medical aid is documented (Tnmed, 2012).

Although Electronic Health Record (EHR) is highly advantageous yet it carries certain potential barriers regarding security and privacy of the records. Since, this system encapsulates host of technology tools i.e., mobile phones and computer devices that increase the risk of widely anticipated data transference among patients, federal agencies, clinicians and organizations and in turn medical identity theft (AHIMA, 2012). Another potential problem is the accessibility to data to a host of stakeholder which was rarely possible in case of books and paper records. Data can be destroyed internally and externally, manipulated, hacked, stolen or damaged hence need of the hour is to address security and privacy concerns of EHRs contemplatively (AHIMA, 2012).

**References**

American Health Information Management Association (AHIMA) (2012). Mobile device security *J Am Health Inf Management Assoc*., 83(4), 50. Retrieved from <http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463>.

Electronic Health Records: Privacy and Security (2012). *Tnmed*. Retrieved from <https://www.youtube.com/watch?v=CgIqWpNK5fo>