Privacy, security and confidentiality research paper example

Law, Security

Abstract

The privacy, security and confidentiality issues have become a primary concern with regards to safe keeping of individual patient health records. With the advent of the automation process and computerization in the management of patient health data and record that is adopted by hospitals and clinics, there is a growing concern how to safeguard individual rights to privacy and how to maintain the security and confidentiality of patient records against unauthorized access. The use of automated systems in the health care setting such as those in the hospitals and clinics has been recognized as an effective tool in improving the efficiency in facilitating patient care with better treatment outcomes. The adoption of informatics has become a valuable tool in assisting the health care professionals to obtain an aggregate data about their patient's health condition that improves patient care outcomes but the use of informatics in the management of patient health records is linked to issues of privacy, confidentiality and security which may be rooted to the misconceptions of their application with respect to safeguarding patient health records. In view of this, this paper will discuss the importance of understanding the terms privacy, security and confidentiality of patient health records within the concept of their usage in informatics and how the latter is valuable in the health care setting in the efficient management of patient health records.

A computer based patient record has become an essential technology in the delivery of efficient patient care. It is recognized as an important infrastructure in information management system that helps the health care professionals to obtain and share aggregate data that are important in

delivering individualized quality patient care (Institute of Medicine, 2010). When hospitals employ the use of automated system in the management of their patient health records, the issues involving privacy, security and confidentiality have become a major concern. The terms security, privacy and confidentiality are often confused and become susceptible to different interpretations. The same confusion is also the cause why many are misguided in raising the issues of privacy, security and confidentiality breach in the use of informatics in the management of health records.

The concept of privacy implies that only authorized health care providers are allowed to view, share and exchange information about individual patient health records for the purposes of delivering patient care and treatment with a defined manner of accessing the same. In short, privacy involves the limitation of access to patient health records only to those authorized individuals in a manner provided by hospital regulations as to how they can access the health records, the time to access them and the scope of information that they can access. Confidentiality on the other hand is defined by Carter (2001) as using the patient data and information strictly only for the intended purposes to which its accessibility is allowed. Any disclosure made that is beyond the intended purpose which is usually only related to the course of care provided to the patient, without the patient consent and knowledge already constitutes a breach of confidentiality of patient health records. On the other hand, security involves the protective measures that may be employed in order to safeguard the patient health records against abuse and unauthorized use that may violate the privacy and confidentiality of patient health records.

When the healthcare industry began embracing the automated system of information management system for health records, concerns about privacy and confidentiality of patient records were raised. Because patient data and information are now accessible through the internet and other forms of telecommunication processes which may be exchanged not only among the health care professionals who are directly involved in the patient care but also between the hospital and health insurance companies and other third parties as well, the security issue is indeed a serious concern that is most likely raised in the use of the information technology system in patient health records. Hospitals on the other hand could not set aside the valuable contribution of adopting an automated, computer based and internet enabled system in the health record management which improves the efficiency and competence of health care professionals in addressing individual needs of patients that essentially improve treatment outcomes and quality care delivery. Among the recognized benefits of an automated hospital system include the speed of the information process that allows health care professionals to promptly address patient needs without waiting for the medical records to be forwarded from one hospital department to another and it enhances the communication process that will help every health care provider to obtain an aggregate patient data in order to deliver a holistic patient care. By an aggregate patient data means that the collective summary of the patient health records that provides a comprehensive overview about the patient condition and treatment process. An aggregate data is a dimension of quality parameters that combine the different parts of a system such as different providers, services, department or patient groups

(Provost and Murray, 2011). The aggregate data obtained from a patient health record may be used as an insightful view about the bigger picture regarding the patient condition that could help the health care providers exercise sound patient care and judgment, thus optimizes patient care and enhances treatment outcomes. Taking this standpoint, it can be said that the use of informatics in the management of patient health records is conclusively beneficial to the health care providers and to the patients as well. The issues of privacy, confidentiality and security may be fully addressed when the proper definition is clearly understood within the concept of the proper use of patient health data in the informatics systems. Legislative protection against the breach of privacy and confidentiality of patient health records are implemented while internal policies, regulations and procedures implemented by the hospital administrators are intended to prevent abuse and limit the extent of purpose and access to which the health data may be used by the health care team and personnel. Limiting access and the employment of a strong computer security measures and internet security protocols are also among the security steps that are employed to ensure that the confidentiality, privacy and security of patient health records are highly safeguarded.

References

Carter, J. H. (2001). Electronic Medical Records: A Guide for Clinicians and Administrators. USA: McNaughton & Gunn.

Provost, L. P. and Murray, S. (2011). The health care data guide: Learning from data for improvement. San Francisco, CA: Jossey-Bass.