Data Incident Management Framework of Electronic Health Record Sharing System In Hong Kong

Ms. RHM Won[1], Ms. CSK Yeung[1], Ms. WY Chan[1], Dr. JA Poon[1], Ms. ELH Tong[1], Ms VH Fung[1], Ms CMM Sum[1], Ms CMK Tam[1], Dr WN Wong[1], Dr NT Cheung[1]

[1]*Hospital Authority, , Hong Kong*

Background

The Electronic Health Record Sharing System (eHRSS) promotes the sharing of health data among various healthcare sectors in Hong Kong. As of June 2019, over 1 million patients and 48,000 healthcare professionals have joined the eHRSS platform. The electronic health data on eHRSS is uploaded and retrieved by various health professionals for patient care purpose. It is therefore essential to ensure the data is complete, accurate and available in a timely manner. One of the challenges is obviously the involvement of vast health professionals with very diverse workflow and technical capabilities using eHRSS. While data standards of eHRSS are established and published, gaps in accurate data sharing could occur due to misunderstanding, human or technical error.

As one of the quality assurance measures, data incident management framework and procedures for eHRSS are established to investigate and respond to potential and actual incident. The scope of data incident refers to incident in which the personal data or clinical data of patient has potentially mixed up, missed, incorrectly displayed or delayed in upload. It does not cover technical system breakdown, security or privacy breach. The goals of the initiative are to control and rectify damage caused by the incident, as well as continuously improve the data quality of eHRSS.

Materials and Methods

The framework involves establishment of governance and processes to handle data incident. An eHRSS Data Incident Response Team is set up to oversee and manage incident in a systematic and transparent manner. Procedures are in place and resources are allocated to the team to enable the works. The progress and result of the incident handling is reported to the eHRSS operation management team on a regular basis.

Data privacy is of paramount importance and legally protected in eHRSS. It is also one of the key considerations when formulating the data incident management procedures. Prudent control measures are introduced throughout the process to safeguard data privacy when sometimes access to and patching of data are inevitable.

Conclusion

In summary, the eHRSS data incident management improves data quality of the platform, and enhances patient care while protecting patient privacy.