BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

Federal Requirements for Sharing Medical Records Jeopardize Privacy

By Jie Wang, LL.M. Candidate 2020 | March 22, 2020

The Office of the National Coordinator for Health Information Technology (ONC) adopted a final rule on March 9, and the Centers for Medicare & Medicaid Services (CMS) issued another rule on the same day, both of which are aimed at improving patients' access to their own medical records.

According to the final rules, hospitals are prohibited from blocking patients' information and are required to send electronic notification to another healthcare facility where a patient is transferred. The final rules also empower patients to access their medical data through any third-party application, such as Apple Health. CMS mandates medical and insurance plans to enable patients to transfer their clinical data to establish a cumulative health record for information sharing purposes.

Despite the empowerment of access to their health data, critics are concerned about patients' privacy. The final rules "fail to protect consumers' most sensitive information about their personal health," Rick Pollack, the American Hospital Association president, commented. "The rule lacks the necessary guardrails to protect consumers from actors such as third-party apps that are not required to meet the same stringent privacy and security requirements as hospitals."

The American Medical Association has warned that the new rules could allow patients who transfer their confidential medical information to third-party apps to get involved in rampant privacy abuse, given the lack of federal privacy protections regarding customer data on the apps. Electronic Health Records (Epic) believes that the rules could result in the misuse of customers' data by, for example, apps exploring more data than patients intended without their consent.

A pamphlet designed by federal health regulators warns patients: "Be careful when sending your health information to a mobile application or other third party" because health providers are "no longer responsible for the security of your health information after it is sent to a third party."

It's possible that these platforms would have no problem using patients' private information for insurance underwriting if the personal information was revealed on these health apps, such as sharing with app developers, affiliate firms, or third-party companies to target the suitable customers in terms of sales and marketing.

Moreover, information of family members will also face sharing risks, as Epic estimates that roughly 79% of healthcare apps are engaging in the data distribution business. For the sake of privacy, patients need well-rounded notification regarding how their data will be utilized and whether app developers will be responsible if they do not comply with what they have promised.