Inherit Data Security Risks of Artificial Intelligence (AI) Enabled Health Systems

Jennifer Ferreras and Philip Shen, School of Technology and Innovation, Marymount University

Abstract

The use of artificial intelligence in healthcare comes with multiple concerns. To sort out the numerous policy-related issues interdisciplinary teams will need to come together.

Informed decisions and patient privacy are two legal concerns that must be addressed. Health organizations must create procedures for explaining Artificial Intelligence (AI) to patients to get informed consent prior to AI implementation. However, currently, the inner workings of AI are a black box as there is a general understanding of inputs and outputs, but not necessarily what occurs in between those processes (Schiff & Borenstein, 2019). Informed consent is an evolving concept. However, every adult and the rational person has the right to choose what to do with their body, according to Judge Cordozo (1914) (Astromske et al., 2021). Comprehension of an AI program may be difficult for both health providers and patients to fully understand (Kerasidou, 2021). The ability to explain a medical procedure is not only important in contract and tort law (which may differ in different countries) but also in data protection laws and is within the jurisdiction of the General Data Protection Regulation of the European Union (Ethics and Governance of Artificial Intelligence for Health: WHO Guidance, 2021).

The use of AI in healthcare raises a number of ethical concerns (Fiske et al., 2019). With the increase in health data collection, processing, and retention, the question of who is responsible for the data utilized in AI applications arises. Vollmer et al., 2020). With tech companies and other private organizations being driven by profit and not health needs, data security regulation requirements continue to be in question. However, to alleviate some of the concerns created by the use of AI technologies, The United States regulatory organization for medical devices, The Food and Drug Administration (FDA) has published guidance regarding AI software regulations for data collection in the medical devices (Content of Premarket Submissions for Device Software Functions. Draft Guidance for Industry and Food and Drug Administration Staff, 2021). Moreover, the development of innovative medical technology needs to stand scientific scrutiny as results need to meet reproducible criteria. Furthermore, laws and regulations addressing concerns with regard to the safety and security of medical devices regarding data security are few, whole laws concerning medical device security and AI are non-existent (Vollmer et al., 2020). Summarily, in the event an AI program or AI-enabled device compromises a patient personal data, there is no established consensus as to who is to be held responsible. (Sullivan & Schwikart, 2019).
References


