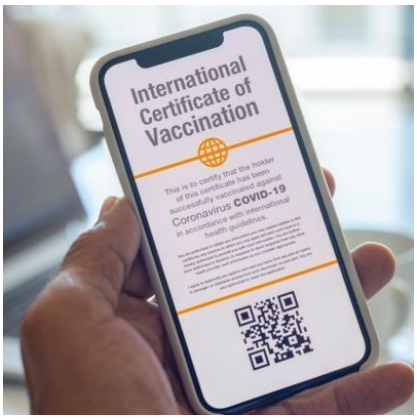
HealthManagement.org
Promoting Management and Leadership

Four Steps to Make COVID-19 Vaccinations Efficient



The United States, where COVID-19 cases continue to rise, is racing to vaccinate as many people as possible to curb further spread of the virus. The inoculation drive, however, poses a major IT challenge as the country's data infrastructure lacks the capacity to efficiently track COVID-19 vaccine distribution and its use (who got vaccinated, what dose, etc.).

You might also like: COVID-19 Vaccines: Need for Global Tracking System

Such kind of monitoring is necessary to make sure that individuals get the recommended number of doses and that enough of the U.S. population – at least 60% to 70% – is inoculated to achieve herd immunity, two healthcare IT experts wrote in an article for Harvard Business Review.

Joram Borenstein, general manager of Modern Work and Security at Microsoft, and Rebecca Weintraub, MD, a faculty member at both Harvard Medical School and Ariadne Labs, have suggested these four steps must be taken to ensure that the U.S. vaccination effort is effective, equitable and with patient privacy protected.

1. Standardise how personal health data is exchanged

It is difficult for the U.S. government to access and manage personal health information, including vaccination records with personal identifiers because of (a) federal and state privacy rules or laws such as the HIPAA and the California Consumer Privacy Act, (b) data silos or lack of interoperability of hospitals' IT systems, and (c) the lack of a single national identification system other than social security numbers. Moreover, not everyone in the U.S. has a social security number and not all healthcare providers organise their data based on them. All these issues can be addressed, the article authors say, by leveraging existing identity verification and management systems from other industries beyond healthcare.

2. Align states' immunisation registries and state and federal reporting analytics

The U.S. has a fragmented system to track vaccine administration. States have their respective immunisation information systems – centralised registries that can electronically exchange data with clinical systems (including EHRs). At present, only 60% of American adults are registered on immunisation information systems (with large variations across states), and not all vaccinators have joined these registries. These gaps in data reporting are aggravated by a recent emergency guidance (issued by Trump administration) to allow pharmacists and pharmacy interns to order and administer COVID-19 vaccinations – note that not all states require pharmacies to participate in their systems.

3. Design immunisation 'passports' that are portable, equitable, and protect privacy

An immunity passport (or proof of vaccination) can be likened to a digitised version of the 'yellow card', the paper-based International Certificate of Vaccination or Prophylaxis that many international travellers carry when visiting high-risk areas of the world. Immunity passports can be designed to ensure privacy and need to be portable so these can be used both within and across borders through a set of common global standards. Another important consideration is the interoperability of such digital passports across organisations (e.g. airlines and hotel chains), governments (both domestic and international), and even healthcare systems. Meanwhile, some airlines plan to introduce COVID-19 health pass apps ('CommonPass') to verify passengers' COVID-19 status. Such pass apps spark concerns around privacy and equity, as vulnerable populations with limited access to vaccination services and smartphones could effectively be denied access to workplaces, restaurants, schools and so on.

4. Address privacy, portability, and cybersecurity tradeoffs

Medical identity theft is one potential problem that could impact a COVID-19 vaccine identity or registry. Bad actors, for example, may steal or fake identities to receive their vaccination sooner than they would under guidelines. Another possibility is the use of fake records that show an individual has received the vaccine when they, in fact, has not (i.e. a fake vaccine certificate). Given such scenarios, it makes sense to consider using existing digital health platforms such as the Commons Project, Simprints, Dimagi, PathCheck Foundation, Yoti and Onfido. As the COVID-19 vaccination effort gathers momentum in the coming months, public health leaders, care provider systems, and pharmacy retailers should work together and implement upgrades to improve the data infrastructure so it supports the efficient and equitable distribution of the vaccine in ways that promote transparency and protect privacy.

Source: Harvard Business Review

Image credit: courtneyk via iStock

Published on : Mon, 4 Jan 2021