IMS Health & Quintiles are now IQVIA™

January 22, 2019

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554

Re: Notice of Inquiry: WC Docket No.18-213, Promoting Telehealth for Low-Income Consumers

Secretary Dortch:

IQVIA Government Solutions Inc., a wholly owned subsidiary of IQVIA, is pleased to provide comment on improving healthcare to low-income populations through the use and promotion of telehealth services. We are a company that has been providing telehealth and mobile health (mhealth) innovations, healthcare program support, data informatics, big data management, and advanced analytics and modeling capabilities to optimize business and clinical processes to government customers since 1999. Our expertise helps government clients with healthcare performance management, health research and analysis, healthcare planning, public health surveillance, technology implementation, and decision support tools.

Our comments for this response focus on the areas of mobile health applications, the incorporation of end user devices, securing patient health data, and funding of end-user equipment.

Mobile Health Applications and Incorporation of End User Devices

Should the pilot program fund equipment used to provide connected care services, such as remote patient monitoring equipment?

Through IQVIA's work with the military, supporting soldiers' care with patient engagement technologies, as well as commercially, enhancing patient engagement for participants in clinical trials, we have seen the value of utilizing patient monitoring devices. Patient monitoring solutions, including our own Patient Engage platform, can monitor, gather and report vital statistics back to the Provider, such as nurses, doctors and specialist. The gathered data can be analyzed for stability, trends and anomalies that can positively impact the health of a patient. Reports can be customized to the needs of the client and can come in various formats like spreadsheets, PDFs and graphs. More robust systems can alert Providers when patient vitals exceed thresholds and immediate action is needed.

While, there are many types of patient monitoring equipment that can address the needs of a telehealth solutions, our recommendation that the focus should be on the utilization of commercial equipment such as blood pressure machines, digital glucometers, scales, physical activity monitors, smartwatches (e.g. Fitbit, Apple Watch), that are readily available. Most of these devices have Bluetooth capability, which allows them to seamlessly link to a mobile device and removing the need for additional steps to capture its data, such as directly plugging into the device. Additionally, these devices tend to be highly user intuitive, therefore more convenient for the patient to operate and use.

Regardless of FCC's decision on the level of equipment to use, equipment management support will be a necessary element for this program. The services provided by an equipment manager, includes a means to distribute, collect, track, maintain, fix and replace monitoring equipment to patients. Additionally, over time equipment become outdated, experience issues, break and are lost. An equipment management vendor will have the necessary resources to handle these and other issues for the program.

What about tablets or smartphones that could be used for the telehealth applications but would also enable access to many other non-telehealth applications?

Tablets and smartphones have become common enough to be considered essential necessities. It is becoming more commonplace for people to replace their land phones, televisions and computers with tablets and/or smartphones. With many wireless providers offering discounted mobile devices, it is more economical for people to purchase smartphones and tablets than other devices. This provides a unique opportunity to expand telehealth technology. Telehealth applications have many advantages over traditional websites. One advantage is that mobile applications allows for direct contact between providers and patients through a quick interface. Whereas with a traditional website, the patient must open a browser, navigate to the site and then enter their credentials. On a mobile device, a patient can merely open the application and log in to get access to their medical data and providers. Another advantage is delivering the ability for providers to directly reach out to patients through push notifications. Alerts, surveys and medical information are a few things that can be sent directly to patients at a frequency that is determined by the provider or as needed. Yet another advantage is remote virtual visits, where a provider can visually and audibly interact with a patient without the patient having to leave their home. More advanced applications, like IQVIA's Patient Engage, will secure all data sent through the platform both in-transit and at-rest using proprietary encryption technology that is stronger than standard security protocols, such as Secure Sockets Layer (SSL).

There are two main approaches to supporting mobile device.

1. *Utilizing an Enterprise Mobility Management (EMM) system*.

   This requires standing up an EMM system and services to manage all mobile devices, including overwriting configurations and policies to protect information on the devices. This approach has its merits in that it allows for full control over securing the devices and can provide remote monitoring of the how the devices are being used and the location of devices. However, using an EMM solution requires incorporating patients' mobile devices into the enterprise system. There may be an issue with patients' willingness to open their devices to corporate control and restrictions. Patients will not want constant monitoring of their nonhealthcare-related activities on their devices.

2. *Offering a secure, Bring-Your-Own-Device (BYOD) solution*.

   This means allowing the patients to use their own devices to securely interact with the provider and their medical data. The advantage is not having to manage devices nor bring them into an enterprise system. Patients are already familiar with downloading applications onto their devices and can easily find a healthcare application in the device application stores. The key is making sure your mobile application can deliver a secure solution, that provides fast and convenient access for the patient. An application can provide remote patient monitoring, virtual patient visits, treatment plans and other healthcare related activities allowing patients to be more involved in managing their health.

Securing Patient Health Data

How can healthcare providers gather comprehensive and informative data on patients participating in pilot projects while remaining HIPAA-compliant?

At the aggregate level, health data can be accessed with the necessary privacy guidelines and regulations in place for both the display and the ability to download to ensure patient level information is compliant with all rules. For example, rules issued under the authority of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulate the use and disclosure of protected health information by covered entities.

IQVIA, as one of the world's largest curator of healthcare data, applies a method of de-identification to a dataset where the risk assessment determines the rules that are applied (preserve, retain, change, etc.) to the different

data elements (Figure 1). This can either be done on a dataset (by dataset basis) and/or in an Extract, Transform, Load (ETL) fashion as data is flowing into a research data lake or data storage location. We employ multiple security layers to "bake" security into the data both by using a common data model or by using our algorithmic tool like that applies context-based heuristics to the dataset.

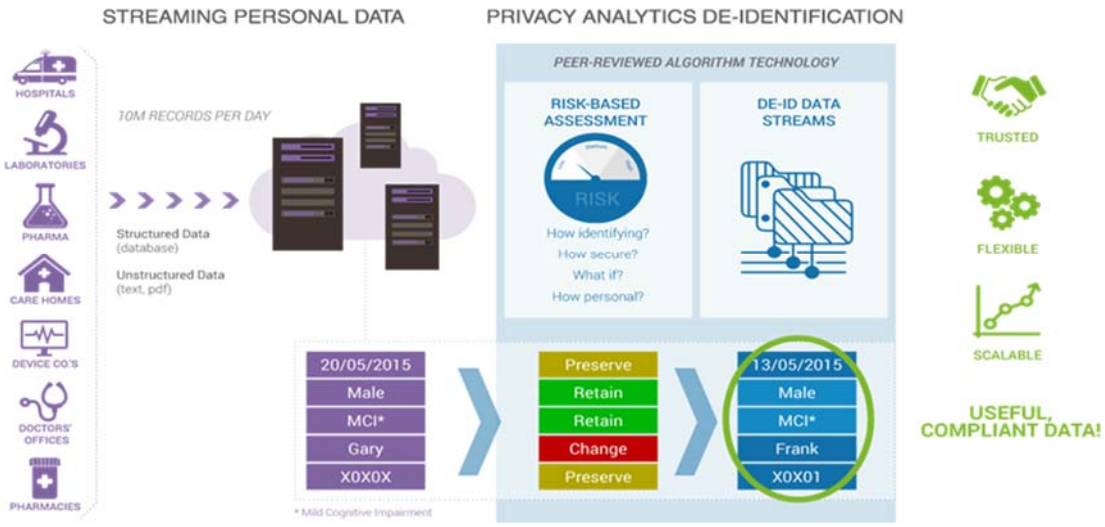

Figure 1: IQVIA data de-identification process

For any study, data security protocols must be established and maintained. As part of the approval process, the study plan is reviewed and approved by an Institutional Review Board (IRB). Patients must have the choice to opt-in or out of study depending on how the pilot is setup as a study. Under the IRB-approved protocols, providers could be allowed patient level data access and would then be accountable for all data use actions with limitations provided for the use of such data.

Should the Commission adopt requirements to protect sensitive information or limit use of information collected during the pilot program?

Both. This is both a data protection and limited data use arrangement.

Are there measures for de-identifying or aggregating patient information that participating health care providers should use?

Each agency has the responsibility to ensure that the Privacy and HIPAA guidelines are adhered to regardless of methods used to de-identify data. Aggregation must ensure that it is performed properly through management of data quality and standardization of the data elements collected. The method in which the data details are provided are also key to the protection of the data (meaning if the data by the nature of disclosure of certain elements enable the re-identification then by default it would not be in compliant with Privacy/HIPAA guidelines. The agency must also have process in place that would be enacted should there be a data breach where information has been compromised.

Should patients participating in the program be required to authorize disclosure of their protected health information?

Yes. There must be information provided to the patients to inform them that the data is being collected and the intended use. This must also be disclosed as part of the IRB submission.

Funding of End-User Equipment

Funding of end-user equipment involves more consideration outside of budgeting to purchase devices and disseminating them to users. Other factors need to be taken into consideration, such as supply chain, inventory management, storage facilities, device maintenance and cost of cellular service. Strung together, those factors can equate to considerable overhead in human resources and financial expenditures.

Additionally, recent numbers from a Pew Survey conducted in January of 2018 (table below), surmises that in all demographic groups there are considerable adoption of smartphones.

PEW Research Survey: Who owns cellphone and smartphones (January 2018)			
	Any cellphone	Smartphone	Cellphone, but not smartphone
Total	95%	77%	17%
Men	95%	80%	16%
Women	94%	75%	19%
Ages 18-29	100%	94%	6%
30-49	98%	89%	9%
50-64	94%	73%	21%
65+	85%	46%	40%
White	94%	77%	17%
Black	98%	75%	23%
Hispanic	97%	77%	20%
Less than high school graduate	90%	57%	33%
High school graduate	92%	69%	24%
Some college	96%	80%	16%
College graduate	97%	91%	6%
Less than $30,000	92%	67%	25%
$30,000-$49,999	98%	82%	15%
$50,000-$74,999	98%	83%	15%
$75,000+	98%	93%	5%
Urban	96%	83%	13%
Suburban	94%	78%	16%
Rural	91%	65%	26%

Utilizing a BYOD solution for this program will present efficiencies by forgoing the responsibilities of providing smartphones or other required equipment as well as avoiding the use of two smartphone devices for many of the participants who already have a personal device. Consideration will need to be made (as well as additional research) to understand data usage for this initiative, as this directly impact the use of personal data and coverage limits established under participants' commercial providers.

Thank you for the opportunity to provide input. We welcome any questions from the FCC and look forward to having an opportunity to provide future support to this program.

Respectfully,

Michael Bruhn
Senior Principal and Director, Real World Insights and Technology
IQVIA Government Solutions Inc.
Michael.Bruhn@IQVIA.com
703-204-3887