

June 9, 2014

Mr. Donald S. Clark
Secretary
Federal Trade Commission
Room H-113 (Annex J)
600 Pennsylvania Avenue, NW
Washington, DC 20580

**Re: Spring Privacy Series: Consumer Generated and Controlled Health Data, Project
No. P145401**

Dear Mr. Clark:

These comments are submitted on behalf of the Medical Device Privacy Consortium, a group of leading companies addressing health privacy issues affecting the medical device industry (the "MDPC").¹ Members of the MDPC manufacture a diverse range of products, from molecular diagnostics to medical imaging equipment to implantable devices, for example. The MDPC appreciates this opportunity to provide input on the privacy and security issues posed by the growth in technologies enabling consumers to generate and control their health data. These comments supplement our submission a year ago in response to the FTC's solicitation of public comment on the privacy and security implications of the Internet of Things.

As we noted in our submission from June 2013, healthcare delivery models continue to evolve and consumers are becoming increasingly engaged in monitoring their own health and making health-related decisions. Consumers who are more engaged in managing their health tend to make healthier lifestyle choices, which in turn lead to being able to live longer, healthier lives. Innovations in technology have played a significant role in enabling patients to monitor their own health and obtain information needed to make informed health choices. As the FTC considers the privacy and security implications of the growth in technologies enabling consumers to generate and control their health data, any consideration of new requirements should always be weighed against the potential risks to innovation.

¹ For further information concerning the MDPC, please visit our website at www.deviceprivacy.org.

It also deserves repeating here the comment in our June 2013 submission concerning the fact that prescription medical devices are already subject to a complex web of Food and Drug Administration (FDA) regulations. The MDPC believes that any further regulatory initiatives in this area should be led by the FDA. The definition of a medical device under the Federal Food Drug & Cosmetic Act is broad and includes any instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other article intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease, or intended to affect the structure or function of the human body. Prescription medical devices can include, *inter alia*, implantable/on-body devices, peripheral/supporting devices, capital equipment, and IT systems. It is also worth noting that both in the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009, Congress has made careful determinations about the application of privacy and security controls in the health arena.

This is not intended to downplay the importance of appropriate protection of personal data, particularly in the health context. -- Indeed, members of the MDPC are at the forefront of the industry in terms of considering how to incorporate privacy and security into the design of products and services and how to appropriately protect personal data. -- Rather, it is to recognize that despite platitudes to the contrary, the protection of privacy and promotion of innovation in health IT may necessarily involve some balancing of societal interests. Elected officials are best positioned to make public policy determinations that involve such a weighing of interests. In the healthcare arena, Congress has expressly directed and authorized the FDA and the Department of Health and Human Services to make those determinations.

Nevertheless, as the Commission examines this issue, it may wish to consider the following points:

1) Notice and individual choice are important principles, but they have much recognized limitations. As noted by the President's Council of Advisors on Science and Technology (PCAST) in its recent report on Big Data and Privacy: "Notice and consent is the practice of requiring individuals to give positive consent to the personal data collection practices of each individual app, program, or web service. Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent." The Commission recognized the limitations of the traditional notice and choice privacy model in its March 2012 report "Protecting Consumer Privacy in an Era of Rapid Change." In that report, the Commission called for "simplified consumer choice" and for identifying certain situations where providing explicit choice is unnecessary based on the context of the interaction or the company's relationship with the consumer. Among such situations where consent can be inferred from the context of the transaction or relationship with the consumer are product or service fulfillment and internal operations such as the use of data for making product improvements. The MDPC supports this framework.

The Commission's 2012 report also, however, suggests that different rules may apply in the context of sensitive data, such as health information. The MDPC recognizes that some personal

data is more sensitive than others, and the rules that apply may need to vary based on the level of sensitivity of data implicated. However, the rationale for the “simplified consumer choice” principle applies equally to both non-sensitive and sensitive data. Where a consumer’s consent can be inferred from the context of the interaction or the relationship of the company with the consumer, a requirement for explicit consent can backfire by leading to notice-fatigue. Instead of a consumer having highlighted for him or her those situations where a proposed data use is likely to differ from the consumer’s expectations, *all* data uses are highlighted and the ironic effect on the consumer is that it is as if *none* were highlighted. The user clicks through (for online/digital interactions) the notice and permission screens often without reading or fully digesting the content. Nevertheless, until the Commission makes clear how the “context of the interaction” standard applies to health data, this is the approach that many companies will feel obliged to follow in order to minimize legal risk.

2) The application of powerful data analytics to health databases can lead to technological innovations and may also enable the delivery of more timely treatments. This is the conclusion of the President’s Council of Advisors on Science and Technology, and it applies equally to traditional patient databases (e.g., electronic health record systems) as to newer consumer health platforms. Data analytics can lead to the design of safer and more effective devices (including software); it can help designers/manufacturers understand how a device is actually being used in practice, so that features can be refined or modified; and it can facilitate the more efficient allocation of capital and other limited resources to those products and services that are of most utility to consumers. Medical researchers can similarly apply regression analyses to large health databases to better understand the relationships among health, demographic, and environmental variables, leading to new medical discoveries. In turn, as new discoveries are made, individual consumers can be alerted so that they can modify their behavior or benefit from some new treatment.

As the FTC examines the benefits and risks of technologies that allow consumers to generate and control their own health data, at the forefront of the Commission’s consideration of risks should be the concept of actual harm. Harms can, of course, come in various forms and sizes, some tangible, some intangible, but not all perceived harms are legally cognizable. The Commission should be cautious about straying too far afield from legislators and judges in granting legal recognition to new or merely speculative forms of injury. Instead, the Commission should focus its efforts on controlling uses of data that have been proven to cause actual harm to consumers, rather than imagined or potential harms. This is particularly true in circumstances such as these where the potential benefits of big data analytics are tremendous.

3) If the Commission wishes to distinguish uses and disclosures of “health” data from other types of data, the Commission needs to clearly define this term. “Health” data could potentially encompass everything from information concerning the manifestation of a disease or condition in an individual, to the predictive risk of an individual acquiring such a disease or condition, to variables, including demographic data, correlated with such risks (e.g., smoker, runner, coal miner, etc.), and on and on. If the Commission seeks to require more stringent controls around “health” data, organizations need clear notice of to what data these controls

must be applied. The Commission should also consider carefully, and articulate, why the existing framework and controls in place under HIPAA, FDA regulations and other provisions of law are not sufficient.

We appreciate your consideration of our comments. Please do not hesitate to contact us with any questions.

Sincerely,

Peter Blenkinsop
MDPC Secretariat and Legal Counsel