Joint Submission in Response to the Competition Bureau's Digital Health Care Market Study

HOFFMANN-LA ROCHE LIMITED
NOVARTIS PHARMACEUTICALS CANADA INC.

September 27, 2021

TABLE OF CONTENTS

Joint Submission in Response to the Competition Bureau's Digital Health Care Market Study

I. INTRODUCTION

Hoffmann-La Roche Limited ("**Hoffmann-La Roche**") and Novartis Pharmaceuticals Canada Inc. ("**Novartis**") (collectively, the "**Companies**") welcome the opportunity to provide this joint submission to the Competition Bureau (the "**Bureau**") in connection with its Digital Health Care Market Study (the "**Market Study**"). We commend the Bureau's continuing efforts to engage with stakeholders through meaningful consultations, particularly in a sector that is of utmost importance to the health and well-being of all Canadians.

As discussed in more detail in the Market Study Notice: Digital Health Care issued on April 8, 2021 (the "**Market Study Notice**"), the Bureau has sought submissions on three broad topics, namely (1) data and information, (2) products and services and (3) healthcare providers. This joint submission is focussed on the first of these topics. In particular, this submission highlights several data and information related impediments that negatively impact innovation, choice and the efficient delivery of healthcare services in Canada.

As recognized by the Bureau in the Discussion Paper issued as part of the Market Study, "the importance of innovation and choice, and the ability to access digital healthcare solutions, has never been more pronounced than it is right now". In fact, the Market Study Notice states that "[t]he COVID-19 pandemic has accelerated the use of digital healthcare, increased the need for technologies and tools to support the delivery of care through digital means, and highlighted the importance of a regulatory landscape that is nimble and responsive to a rapidly evolving sector". Removing the impediments identified in this submission will foster new and more efficient ways of providing increasingly necessary digital healthcare to Canadians.

II. DATA AND INFORMATION

There are several regulatory and non-regulatory barriers that prevent the access, use and sharing of high-quality digital healthcare data to the detriment of Canadians. As discussed in more detail below, these barriers relate to a lack of access to data, which is the result of, among other things, the lack of a harmonized privacy framework in Canada that takes into consideration the realities of our current technological and commercial world; minimal open access to data; and data portability issues stemming from the absence of unified data standards. Reducing these barriers will encourage competition and innovation in the digital healthcare sector.

Access to Data

Increased and more timely access for biopharmaceutical and life sciences companies to high-quality healthcare data would lead to increased innovation in the digital healthcare sector. For example, timely and increased access to healthcare data would enable biopharmaceutical companies to provide more value to the public in the form of new and better drugs as well as higher quality, personalized and more targeted patient care. While we recognize that there may be a tension between access to data and privacy, any such tensions can be addressed in some instances by, for example, providing for the disclosure of aggregated, de-personalized or anonymized information. In this regard, while in some medical research areas access to anonymized information would allow companies to provide the public with a portion of the full benefit that could be realized from having access to personalized information, such companies would not be able to target specific patients with solutions for them. Additionally, in some other research areas,

as discussed more fully below, appropriate access to individual level data is required in order for biopharmaceutical and life sciences companies to provide essentially any value or new innovations to the public.

In the absence of a proper framework for the sharing of healthcare information, biopharmaceutical and life sciences companies are spending a lot of resources (both monetary and otherwise) on third-party organizations that collect and aggregate such information. This is a very inefficient process that negatively impacts the work that biopharmaceutical and life sciences companies are currently doing, as these resources could otherwise be put directly into research and development, as well as other activities that directly benefit consumers. If information was more readily available to biopharmaceutical and life sciences companies, these companies would be able to do their work more efficiently, including reaching a greater number of patients more quickly.

Moreover, due to the decentralized and fragmented framework for the sharing of healthcare information, which relies on third-party intermediary organizations, the quality of the data that is made available to biopharmaceutical and life sciences companies is being negatively impacted and significant timing delays are being created that in turn lead to delays in proper care for patients. Higher quality data allows biopharmaceutical and life sciences companies to create better and more tailored products for consumers. The use of third-party organizations to collect and aggregate data also increases the amount of time required for companies to develop products, and delays products and innovations from reaching the market in a timely fashion. This is particularly of concern in the healthcare industry, as timely access to new innovations can be critical as health crises often require a real time response.

Various examples demonstrate the benefits that could arise from increased access to health-related data and the potentially serious consequences that may result where such access is not provided:

- **COVID-19 Tracking**: Countries around the world, including Canada, are using apps to monitor people for contact tracing purposes. Countries like South Korea and Singapore, which collected and made available more data from these apps, were able to implement proactive measures (such as contract tracing) which yielded successful results in curbing the spread of COVID-19.

- **Artificial Intelligence**: The potential for artificial intelligence to improve healthcare is revolutionary. However, without enough quality data, smart algorithms simply cannot function as intended. For example, most smart algorithms require multiple, large sets of data in order to train, and then test/validate an algorithm. Without multiple, high quality data sets it is impossible to fully review an algorithm for bias, precision and accuracy. These concerns arose in the context of the Flu Tracker previously launched by Google, which aimed to predict flu outbreaks. However, in 2013 it failed at forecasting that year's peak by 140%. Lack of trustworthy data was among the causes of this failure, resulting in Google halting this innovative product in 2013.

- **Targeting Unique Populations**: Access to more data would allow private companies to quickly identify population segments where more or different resources, research or medicines are required. This includes unique populations where companies would not have otherwise realized that consumer demand exists. Moreover, if there was increased access

to open data, it would allow private and public entities to collaborate more easily and efficiently. For example, it would allow public bodies which have identified at risk populations to share their results and underlying data with private institutions which have the resources and processes in place to quickly design and manufacture product solutions for these populations. Access to data to identify at risk population segments would also allow for identification of which institutions are best situated to set up clinical trial sites accessible by those patients.

- **Submissions for Drug Approval:** Health data which is held by provincial bodies is required by private companies in order to make submissions to regulators for approval of new medications. However, due to inefficient data privacy and data sharing frameworks, the data that companies will receive in response to such a request is usually 18 months to two years old. Such data is often much less useful by this point, especially in fast moving therapeutic areas such as oncology, and will not provide insight into current issues and health outcomes. This delays patients from having access to appropriate medicines. This also disadvantages Canadian companies as compared to international competitors, which may have better access to more timely data, and creates barriers which hamper Canadian companies (and Canadian consumers) from being at the cutting edge of drug development. This disadvantage as compared to other countries and companies is also a contributor with respect to the lack of economic growth for Canada in this sector.

Moreover, while fully anonymized or aggregated data may allow private companies to engage in some types of medical research, individual, pseudonymized data is required in some cases, and anonymized or aggregated data will simply not be sufficient. For example, fully de-identified, anonymized or aggregated data does not allow for insights to be generated with respect to genomic testing. Similarly, longitudinal health studies (which follow a cohort and have repeated observations of each patient over time) are required in many cases to properly review and analyze long-term health outcomes. In order to carry out longitudinal studies, coded patient data is required and fully anonymized or aggregated data would not be sufficient. In this area, there is a need to look at individual level data in order to properly inform drug development. Access to individual, pseudonymized data is not at odds with privacy considerations, and a balance can be achieved which protects individuals but also allows private companies to develop better and more targeted products and services that would ultimately provide greater benefits to consumers.

As discussed by Ann Cavoukian (previous Privacy Commissioner for Ontario) in reference to her Privacy by Design conceptual framework, privacy should not be considered a zero sum game, and that, moreover, privacy can still be an integral consideration while not "diminishing functionality".[1] In other words, privacy can "[seek] to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made".[2]

---

[1] Cavoukian, Ann, "*Privacy by Design: The 7 foundational principals"*, (January 2011), available online at www.privacybydesign.ca.

[2] *Id.*

Lack of Harmonized Privacy Framework

It is widely-recognized that dynamic competition, including innovation, is the most important type of competition.[3] However, the complex and often conflicting privacy legislation in Canada negatively impacts innovation in the digital healthcare sector. In fact, there are significant differences among the federal, provincial and territorial privacy regimes, which, in turn, create different standards, potential conflicts and lack of predictability. For example, federal legislation (namely, *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**")) will apply in some provinces in addition to provincial private sector privacy laws, but in other provinces, including Alberta, British Columbia and Quebec, private sector laws may apply instead of PIPEDA. Moreover, the various statutes differ with respect to even the most basic issues, including with respect to the definition of "personal health information". Complex and differing rules regarding consent also create undue difficulty. This means that, for example, it is currently inefficient and cumbersome for biopharmaceutical and life sciences companies to obtain consent from patients in each province and territory (as is required in order to obtain a fulsome set of data), which creates unnecessary barriers and negatively impacts the ability of such companies to conduct medical research. In addition, for each federal, provincial and territorial jurisdiction, health care custodians must comply not only with general privacy laws, but also with additional healthcare privacy laws. This adds an additional layer of complexity for biopharmaceutical and life sciences companies which participate in partnerships with healthcare professionals and other health information custodians.

Simply put, complex and differing rules, and different interpretations of the rules, create barriers to the sharing of data across the country and internationally, which negatively impacts research and innovation. Moreover, the interpretation and application of privacy legislation by various privacy commissioners and officers is often inconsistent and unclear, which leads to further difficulties in complying with the regulatory regime.

In contrast to the complex and often conflicting privacy legislation in Canada, the United States privacy framework includes national standards that apply to healthcare information. In particular, the *Health Insurance Portability and Accountability Act of 1996* ("**HIPAA**") is a federal law that modernizes the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addresses limitations on healthcare insurance coverage. This results in predictability and helps build trust, which, in turn, promotes innovation in the digital healthcare sector in the United States. The digital healthcare sector in Canada would benefit greatly from a harmonized framework for the treatment of healthcare information that includes clear and consistent rules related to patient privacy, data protection and consent.

Similarly, the European Union's *General Data Protection Regulation* ("**GDPR**") creates a privacy regime which applies to all Europe Union Member States. The GDPR sets out rules regarding personal data privacy, collection, use, processing, storage and security. The GDPR replaced various different privacy protection regimes across the Member States and both harmonized and modernized privacy law in the EU.

[3] See, for example, *The Commissioner of Competition v. The Toronto Real Estate Board*, 2016 Comp. Trib. 7, Reasons for Order and Order at par. 712.

There is a concern that Canada is not keeping up with other international jurisdictions, such as Europe, with respect to modernization of privacy law. As noted above, this means that Canadian companies are at a competitive disadvantage internationally. Moreover, this also means that multinational companies are less likely to carry out medical research and clinical trials in Canada – meaning that Canadian consumers will not be included in, or benefit from, such cutting edge medical research in a timely manner. This can create a negative feedback cycle which could end in even internationally considered "standard" care not being available in Canada.

While a harmonized set of privacy laws in Canada is an important first step, global harmonization should be the ultimate goal. Harmonization with other jurisdictions would allow data sharing on a global level, which would be especially beneficial in certain areas, such as with respect to rare diseases, where limited patients on a country basis means access to global data is important and could lead to huge benefits for Canadians. Notably, recent proposals in Canadian privacy legislation already reference a GDPR like structure.

Moreover, due to the geographically large size of Canada, and the fact that its population is relatively small and dispersed across the various provinces and territories, it is often (if not always) necessary for biopharmaceutical and life sciences companies to collect data from persons located in all, or many, provinces and territories. Interprovincial data sharing will allow access to large scale data across a diverse population, which will in turn foster an innovative environment.

We understand that the Bureau does not intend to evaluate substantive issues pertaining to the privacy of digital health data and information as part of the Market Study. However, a more harmonized framework for privacy laws (regardless of the substance of these laws) would benefit numerous stakeholders and would bring about greater innovation, choice and access to digital healthcare across the country.

Outdated Regulatory Framework

In addition to the concerns regarding harmonization discussed above, the regulatory framework is outdated and in need of modernization. This legislation was introduced prior to the invention of the iPhone – and has not been updated. There have been significant changes since these laws were enacted, not only in the way consumers share and access data, but also advances in data protection technologies which should be considered as potential alternatives or enhancements to the current notice and consent framework which Canadian privacy legislation is based upon.

Modernized privacy laws should take into consideration new technologies, including the ability to use pseudonymization[4] or de-identification as opposed to full aggregation and anonymization to protect data, and the potential use of other Privacy Enhancing Technologies. This would allow

[4] Pseudonymization is a method that allows you to switch the original data set (for example, e-mail or a name) with an alias or pseudonym. It is a reversible process that de-identifies data but does not require aggregation, and allows the re-identification of data later (if necessary). This reidentification is not possible without access to a separate set of data that is held separately. Pseudonymization is a recommended data protection method in GDPR, and several GDPR requirements which normally would apply to personal data are relaxed for pseudonymized data. For example, pseudonymized data may in some cases be used by the controllers of that data for purposes other than the purpose for which it was collected (see GDPR, Article 5, 6(4)(e)).

consumers to trust that their privacy is being protected, while allowing private and public health sector participants increased access to data.

The existing regulatory framework is also not aligned with current commercial realities or expectations. For example, it includes a significant number of direct-to-consumer restrictions, which, in turn, limit what would otherwise be very beneficial consumer interactions (such as the ability of biopharmaceutical companies to identify themselves on social media). There is clearly no rational basis for many of these restrictions, as the information is already accessible through other (albeit less efficient) channels.

Finally, there is a concern that the existing regulatory framework is undermining trust in the digital healthcare space, particularly given the considerable number of data breaches over the past few years.[5]

Proper protections to prevent similar breaches from occurring in the future, along with increased, meaningful, transparent enforcement of privacy laws which already exist, are necessary to regain the trust of patients and unlock the benefits associated with digital healthcare. Meaningful enforcement does not simply mean "more" enforcement, but includes clear guidance regarding rules and penalties, increased public transparency with respect to enforcement and investigations, increased oversight by regulatory bodies, and increased accountability for private organizations.

Meaningful enforcement coupled with modern privacy laws which take into consideration new technologies would help facilitate feelings of trust for consumers regarding their privacy being protected, without unduly limiting data sharing and sacrificing the ability of industry participants to innovate.

Data Interoperability and Portability

Increased data interoperability would increase the amount of data that is available to a company, which would in turn increase a company's ability to research and innovate. This would ultimately lead to better products and services for consumers.

For example:

- Increased data interoperability may have allowed various private companies, local and provincial public health authorities, as well as various provincial, state and international governments to share data regarding COVID-19 research and vaccine development, which may have lead to faster development of vaccines, improved access to vaccines, more individualized vaccines (for example, aimed at persons with allergies or other complications which currently restrict them from receiving a COVID-19 vaccine) and perhaps even shorter lock-downs in some jurisdictions.

[5] See, for example, the 2017 Equifax data beach and the Fédération des caisses Desjardins du Québec 2019 data breach.

- Some countries, such as Finland, Estonia, Iceland, Denmark and Israel, have standardized medical records. In particular, Estonia and Israel were able to give health outcomes data to Pfizer to assist in COVID-19 vaccine distribution.

Better interoperability would also decrease barriers to new entrants, as it would increase their ability to access and use data and hence innovate and compete with existing incumbents. New entrants may not have the resources to collect data independently, and may rely on purchasing or otherwise procuring data from third parties. Where technological barriers deter entrants from being able to make use of data collected and stored by third parties, this drastically decreases their ability to undertake the research required to develop new and innovative products and services.

Unified data standards are required in order to increase data interoperability and portability. These data standards relate to, among other things, the format in which data is stored and the definitions of data variables. Unified standards would allow entities to more easily access and use data collected by other entities. Currently, even where privacy laws would allow the sharing of data between entities, data interoperability and lack of unified data standards create a technologically barrier that is unduly costly (or impossible) to overcome.

Currently, there are no federal unified data standards, and there are no federal rules or requirements for public or private institutions to adopt any particular data standards. While there are some provincial guidelines, lack of federal standards leads to fragmentation of data and decreases the ability of companies to access and harness data for purposes of research and innovation. Collaboration with respect to data standards, increased requirements for interoperability and encouraged adoption and harmonization of existing data standards and guidelines is key to unlocking the value of healthcare data.

While there are multiple private entities, such as the CIO Strategy Council and Infoway, which are working to develop usable data standards, there is a need for centralized leadership to connect the work of these institutions, to further progress this work, and to implement rules and requirements which will guarantee both public and private organizations adopt these data standards.

The federal government is in the best position to provide this leadership for multiple reasons. First, a large portion of the personal health data that exists in Canada is already controlled by public institutions, through the public healthcare system. As such, it is of paramount importance that the data standards are adopted by public health institutions, and that there is coordination between provinces in this regard. Moreover, the federal government is more appropriately situated to ensure organizations adhere to mandated data standards and interoperability requirements. Additionally, the federal government is in a better place to push the benefits of data standards even further by engaging with other countries with an eye towards *international* data standards. Such standards would advance the goal of international data interoperability, which would lead to the same consumer benefits as described herein, but on a global scale, and would lead to increased benefits to Canadian consumers who would be able to benefit from research undertaken on larger sample populations.

However, the government should also engage with the private sector in implementing the adoption and harmonization of existing data standards and interoperability requirements. This would allow the government to not only leverage the work already completed by private institutions (such as

the CIO Strategy Council) in this area, but would also ensure the adopted data standards meet the needs of private sector companies as well as the public sector. In order to create the most benefits, data standards need to tie together all health information databases, which would include both private and public databases. Moreover, collaboration with multinational private organizations would allow the government to further progress the goal of global alignment of data standards. As such, communication and engagement between the public and private sector is imperative.

Proprietary Data and Open Access

It is not uncommon for public and private organizations to share the healthcare data they collect only with their subsidiaries and partners. While this may be profitable for the organizations in question, it adversely affects innovation by biopharmaceutical and life sciences companies and other entities that do not have access to such information.

Currently, large incumbent organizations are in the best position to collect and curate large data banks. These organizations do not only use these data banks for their own research and development purposes, but also sell data to third parties, or charge a fee to undertake research on behalf of third parties. This not only means that these organizations are profiting from personal data in a manner that does little to benefit the consumer, but it also puts them at a competitive advantage as compared to smaller entrants.

In order to mitigate the negative effects on competition which these practices create, concepts of data interoperability (as discussed in more detail above), open access and data mobility need to be carefully considered. Even where regulatory barriers and interoperability barriers (each as discussed above) are addressed, if there is no push towards open access of health data, many of the benefits discussed herein will be limited, and the ability of smaller entrants to compete will be hampered.

An open access approach to health data which reflects the open data/open science principles seen in other fields would allow more organizations to access data at a reduced cost. Most importantly, this would allow new entrants who are not able to collect sufficient data independently to access the data required for research and development purposes at little to no cost – which would help to level the playing field between these entrants and the incumbents currently controlling and monetizing data. This would ensure that the resources of organizations are allocated to research and development, and other activities that directly benefit consumers, rather than unnecessarily spending these resources on access to, or creation of, data. This would not only benefit new entrants in the private space, but would also assist academic institutions, which often struggle to access data.

More generally, open access to data would lead to increased innovation by *all* companies (incumbent and new entrant alike) as improving access to external data sets increases both the incentive and the ability to innovate. First, as noted above, open access would remove a barrier to entry to new entrants. Additional competitors in the market would mean a heightened need for all market participants to compete on the merits and accordingly would necessitate increased innovation from all companies. Second, access to additional external data sets would allow all companies to undertake more research (at a reduced cost) leading to more optimal and innovative products for Canadian consumers and economic growth for the country.

II. CONCLUSION

The Companies appreciate the opportunity to provide this joint submission in response to this Market Study. We would be pleased to discuss any aspect of this submission in more detail if that would be helpful.