Introduction

In an earlier environmental scan, we defined patient-generated health data (PGHD) as as "health-related data created, recorded, or gathered by or from patients (or family members or other caregivers) to help address a health concern", using the definition provided by The Office of the National Coordinator (ONC) for Health Information Technology (1). In the concluding paragraph of that paper, there was ambiguity as to whether PGHD was considered to be personal health information (PHI). If PGHD does indeed fall under the umbrella of PHI, does this essentially mean that PGHD can be understood to be governed under the same legislatures that govern PHI?

The Information Privacy Commissioner (IPC) of Ontario defines personal health information as "identifying information about an individual in oral or recorded form" (2). According to this definition, if the identifying information is related to an individual's health care provision, their health care payment and eligibility, or their physical and mental health (including health history), it is considered to be personal health information (2). Given this definition, PGHD does seem to fall under the umbrella of personal health information. However, this raises more challenges. Personal health information is protected by different legislatures – some of which are state-specific, country-specific, or even multi-country specific.

This paper will seek to understand the kinds of legislature that govern personal health information and the applicability of such laws to patient-generated health data. More specifically, we hope to discover how the language around legislature for PHI addresses the various concerns and challenges related specifically to PGHD and whether current legislature should be amended to include patient-generated health data. If there are unique considerations that should be taken into account for PGHD, it may be beneficial to understand the principles and values associated with its collection, storage and use. Therefore, a second purpose of this paper is to determine whether there are principles of PGHD that currently exist, and how these principles have been put into practice. The previous paper emphasized that various stakeholders are affected in one form or another by PGHD, including patients and their caregivers and family members, physicians, developers, policymakers, and researchers. It will be of particular interest to determine the group responsible for developing these PGHD principles.

While there are numerous laws that govern PHI or personal data in particular, this paper will focus on three main ones – one at a state level, another at a national level, and finally one at a multi-nation level. The first is the Personal Health Information Protection Act (PHIPA), created in 2004, for the province of Ontario in Canada. The second is the Health Insurance Portability and Accountability Act (HIPAA), created in 1996, for the United States. The third legislature is the General Data Protection Regulation (GDPR), established in 2016, for all countries in the European Union (EU).

In the previous paper, we described the various methods of collection for patient-generated health data. This paper will essentially be focusing on how current legislatures apply to a specific method of collection – PGHD collected and stored on mobile apps – though we acknowledge the importance of other tools, like wearables and home monitoring devices. Since there are more than 100 000 health-related mobile apps available on Google Play and the Apple App store (3) it would be interesting to determine how current legislatures affect them and the consequences of that effect. This paper will additionally be focusing on how the influence of personal data legislatures on PGHD affects patients and

providers, though the paper will also briefly discuss other stakeholders like developers, researchers, and policymakers.

Personal Data and Personal Health Information

Canada

In Canada, personal data is governed under the Personal Information Protection and Electronic Documents Act (PIPEDA) at the national level (3,4). However, since the law relates to personal data in general and is not specific to health information, many provinces within Canada, such as Ontario, have province-specific legislature for health information (4). Provinces are able to enact legislature to specifically oversee health information if they are structured similarly to PIPEDA (5). It should be noted that like Canada, legislature overseeing personal data in EU countries are also not specific to health information. However, like Ontario, legislature in the United States is specific to personal health information.

The Personal Health Information Protection Act (PHIPA) outlines the rules that govern PHI, including how to "collect, use, and disclose" the information (5-7). These rules apply to 'health information custodians' and includes both the individuals (healthcare providers) and organizations (hospitals, nursing homes, pharmacies) involved in healthcare delivery (7). This legislature also applies to 'agents' of health information custodians, who are individuals that can act on PHI, with the express permission of the health information custodians – including employees and contracted individuals (7).

United States

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) outlines regulations for safeguarding personal health information (8). This legislature applies to 'covered entities' and while it differs in its name, it is similar to health information custodians covered under PHIPA in Ontario. Covered entities include individuals and organizations involved in the operations, treatment, or monetary transactions of healthcare (9,10). This include health care providers (which, in the United States context includes hospitals and clinics), health plans, and 'healthcare clearinghouses' which are involved with payment processes (8-10). The legislature is also applicable to 'business associates' which, again although it differs by name, is similar to agents covered under PHIPA in Ontario. Business associates are individuals, vendors, and organizations who been contracted by a covered entity for a service which requires them to have access personal health information (9-11).

Mobile Applications

Understandably, there are many differences between the legislatures governing PHI in Ontario and the United States. However, the entities that their regulations apply to are similar in nature. This paper will now take a deeper look into how these regulations affect PGHD, specifically its association with mobile health apps.

As mentioned in the previous paper, one tool that has emerged and has been particularly popular for storing PGHD are mobile health apps. These apps are available for a variety of different purposes and

facilitate individuals to collect health-related information including (but not limited to) physiological data, physical activity, diet, and changes in cognitive behaviours. Mobile health apps act a medium that patients can use to store their data. This tool essentially helps them keep track of their health and monitor their conditions. These devices enable individuals to collect real-time data about themselves by noting important symptoms and other changes in their physical and mental health. Mobile health apps may help patients adhere to their treatment plans and they may hold information that is crucial in helping healthcare providers understand how their patient's health is changing.

On a larger scale, the challenge is taking the useful information generated by patients and making it available for a higher purpose. This includes individual information used for different research initiatives so that the accumulation of PGHD collected from numerous patients can be used as evidence to inform, reach, and help a larger population. At an individual level, however, the challenge is ensuring that the information patients have generated is useful for themselves – for their care and their health.

As discussed earlier in this paper, PGHD essentially fits under the umbrella of personal health information. The health information by itself does not necessary count as PHI, but when paired with identifying information, it certainty fits the scope (10). For instance, if there are heart rate measurements, but that information is not linked in any way to identifying information (e.g. name, date of birth), then that information would not count as PHI. However, if these readings were linked with personal identifying information, like in health records or EMRs, then it falls under the umbrella of PHI.

This is where things become confusing. Intuitively, one would think that sharing health information from a mobile app with your physician, who then manually incorporates or uploads that information on a patient's record, would be protected under the same laws that govern PHI. However, this is not necessarily the case. Patient-generated health data falls under a gray area. When creating their products, app developers may not have been necessarily thinking about legislatures governing PHI, such as PHIPA and HIPAA. In fact, if the ultimate assumption was that this information was only going to be stored on the mobile device and that only the device owner will have access to that information, there would be no need to worry about legislatures such as PHIPA and HIPAA. App developers may have simply relied on protections such as password-protected mobile devices or authentication via fingerprints to act as their security measures (4). Unless app developers are specifically contracted by health information custodians (in the Canadian context) or covered entities (in the U.S context), then PHIPA and HIPAA legislature cannot be applied to them (4,12).

It is not farfetched to assume that once patients have shared their PGHD with their providers, and that information is incorporated in their medical records, that privacy and confidentiality is ensured and their PHI is safeguarded (13). Similarly, if a provider recommends a healthcare app or if a patient shares information from a mobile health app that the provider uses, one may make the assumption that there is some kind of legislature (like PHIPA or HIPAA) safeguarding the information or ensuring oversight. In some cases such an assumption may be true, but certainly not in all and it may be difficult for both patients and providers to know when it is the former and when it is the latter.

<u>Mobile Apps, PGHD, and Personal Data Legislature</u>

In the United States, the Office for Civil Rights has developed a portal to help mobile app developers understand how their technology may be affected by HIPAA. One such resource includes scenarios of when mobile apps are required to be HIPAA compliant. In summary, mobile apps are not beholden to HIPAA if:

1. The individual simply downloads the app and populates it with their health information,
2. The individual populates her mobile app with information from an EHR (via a patient portal accessed through her computer and then uploaded to her mobile health app);
3. An individuals downloads an app that is recommended by her provider and uses the information to create a summarized report for her physician,
4. At the patient's request, there is an exchange of information from the mobile app to the EHR, which both the provider and the patient could view based on an interoperability arrangement between the healthcare provider the mobile health developer (12).

Even though a patient is inputting health data into a mobile health app (sometimes at the recommendation of the providers), and this information is sometimes available to be viewed by a provider or even integrated into the patient's EHR, mobile app developers are not beholden to HIPAA unless there is a formal contract between the developers and the providers. In the last scenario, the mobile app only facilitates the exchange of information between the patient and the provider when the patient requests it, but since the provider has not contracted the developer, they are not beholden to HIPAA. So, when are mobile health app develops beholden to HIPAA? Only when they are specifically contracted for a service and become a business associate (12).

While a similar resource does not yet exist for Ontario, it is probable that PHIPA applies to mobile apps in a similar fashion, given that this legislature is only applicable to health information custodians and their agents. Ultimately, since PGHD is not governed under legislature like HIPAA, that puts patients at risk at having their data re-identified (that is, their health information is linked to their identities). These potential risks lead to concerns that if certain medical conditions become public knowledge, one may be denied job advancements/opportunities and health benefits (14).

In essence, HIPAA does not prevent covered entities from receiving PGHD, but it cannot necessarily do enough to safeguard it either (15). This does not mean healthcare providers cannot use PGHD as part of their practice. It only means they must be extra careful, as there are is no concrete oversight (16). They are still able to incorporate PGHD, but must be extra cautious to uphold the privacy and confidentiality of their patients. However, as mentioned in the previous paper, because there is no standard regulation overseeing the collection, use, and sharing of PGHD (1,14), providers may be reluctant to incorporate it into their practice for fear of breaking the law or being held liable for either acting on inaccurate information or not acting due to uncertainty (1, 13, 14).

In the Canadian context, not only are mobile health apps not governed under PHI legislature, they are not governed under Canada's Medical Devices Regulations either, as these rules were created before the advent of mobile health apps (4). Essentially, there is little or unclear regulation and oversight over mobile health apps. Similarly, in the United States, HIPAA does not apply to developers of medical devices (including mobile health apps) or to patients (16). To add to the complexity, even if mobile app developers choose to follow specific PHI legislature, there is no clarity as to which one they would follow. Intuitively, one may think they would only be beholden to laws in their country of origin. However, they would need to consider whether there are individuals outside their jurisdiction using the app and the applicable laws in that (4).

Although this paper focused on mobile health apps, it is likely that many of the same challenges and complexities can be applied to other tools such as wearables, which again likely do not consider PHI legislature when developing their products.

There are more challenges than simply ensuring the privacy and confidentiality of patient-generated health data. Since it is their own data, and not information created by their health care providers, patients should be able to access this information any time they choose. They should also be able to add to this information, and make any corrections to inaccurate information as needed. As mentioned in the previous paper, patients are already able to request a copy of their medical records and some even have the ability to view certain (but not necessarily all) information online via a patient portal. Sometimes, there is even a section where patients could write in notes (17). However, these notes, some of which pay be viewable by the physician, are only for the patient his or herself; they cannot make actual changes or additions to their medical information (17). However, PGHD, ideally, should work differently. So while the scope of this paper focuses on the confidentiality and privacy aspect of PGHD, there are many more challenges and hurdles invovled, as alluded to in the previous paper.

European Union and Personal Data

Thus far, this paper has discussed legislature in the United States and Canada that were created more than a decade ago. Since the use of mobile health apps is a newer trend, it is understandable that such legislatures does not wholly encompass the security and confidentiality concerns related to patient-generated health data. However, the legislature protecting personal data in the EU is more recent. The EU General Data Protection Regulation (GDPR) of 2016 was fully enforced in Mid-2018, replacing its old legislature the Data Protection Directive of 1995 (18). Unlike PHIPA and HIPAA, the GDPR is not specific to PHI, but applicable to all personal data (similar to Canada's PIPEDA). The GDPR was based on a set of old, but still relevant, principles (Appendix A) created by the Organisation for Economic Co-operation and Development (OECD), in their published document, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (19, 20). This document was endorsed by both the U.S and the EU. While still holding true to old principles, the EU's new legislature is meant to include updated information that would be applicable to technology, including mobile health apps (19). This means broadening the scope of identifying information so that "data processing" (i.e. personal data that is stored, analyzed and shared) now includes one's IP address and genetic sequence (18, 21).

The most promising aspect of the GDPR is that individuals will have greater rights (Appendix B) about what their personal data is being used for, whom it's being used by, and why it is being used (21). The new legislature is patient-centred (22) are similar to rights found in other legislature, such as PHIPA in Ontario (Appendix C) (23), but the GDPR also includes additional rights. However, as the EU GDPR has only been in affect for about a year now, it is too soon to determine how it will affect patient-generated health data.

Thus far, some difficulties have been noted, as 'data controllers' (i.e the EU equivalent of covered entities for all personal data) are struggling with the new GDPR rules (24). It has been noted that in the health care setting, many still use paper-based methods. Citizens in the EU have always had the right to access their data, but now they have the "right to be forgotten" (18) which leaves little clarity as to whether it is appropriate for health care entities to delete old files (24). Furthermore, it is unclear what happens to data was previously governed under the old legislature and the data that is now governed under the GDPR. For example, some researchers are unclear as to whether their study participants have to undergo another consent process and they are unsure about what happens to the data that has already been collected (24).

As new technology is being developed, such as medical devices, they can be designed from the outset to be GDPR compliant. The issue arises with devices that have already been designed and is in use. Medical

Devices in the EU are regulated by separate legislature (the same as in Canada) and developers will have to find a way to ensure they remain compliant to all applicable laws, which creates further complications (especially, if in the case of the EU, the medical devices regulation has also been recently updated) (24). Returning to the issue of previously developed technology, as with Canada and the United States, mobile apps and wearables are unregulated entities, and were not beholden to any personal data legislature. The former fact remains true, only now EU mobile apps must be compliant with the GDPR (24). As a result, mobile health apps may have to go back and redesign their products to comply under the new security measures, or it may mean that data controllers will be more reluctant to use such technology over confusion over whether a product is GDPR-compliant. The situation is especially complicated if you consider that not all mobile health apps and wearables are developed within the EU countries. Again, as the GDPR only recently came into affect, it is too soon to determine how these challenges will be addressed.

The GDPR is more patient-centric and ensures individuals have more rights over their personal data than they previously had. It is a step in the right direction, but it seems as through there are many more challenges that remain. Nowhere in the document does it refer to PGHD and how such data may be differentially affected by the GDPR. The challenges outlined above related to wearables and mobile apps make that evident – and since such devices are prime devices to store and share PGHD, it is possible that further work in this area will be required.

It is up to these countries to determine how to tackle the issues of patient-generated health data. As it is health information that could be potentially be linked to an individual, it makes sense to include it under the umbrella of personal health information. As such, it may more logical to amend current frameworks and legislature that govern PHI than to create a new one just for PGHD – but that is at the discretion of policymakers in their respective countries.

There are many similarities between the legislatures discussed above. All three outline that individuals have the right to access their information, they are able to correct any information that's inaccurate, they must either be notified when their PHI is being used or instruct that their information should not shared with others, and finally, they outline how personal data can be used for research purposes. While PHIPA and HIPAA do not directly govern PGHD and its associated technology (mobile apps, wearables) in many cases, the EU GDPR is applicable to technology, though its affect on PGHD remains to be seen.

PGHD Principles

As previously mentioned, the EU's GDPR is based on principles that were created by the OECD. Many legislature are based on previously created principles and frameworks that act as a guide or model to help policymakers develop their laws. At this time, this paper will discuss the current principles that exist for PGHD and investigate who was involved in creating those principles. Such principles could be used as a guide of how PGHD should be collected, stored, and shared – or determine whether there are gaps in these principles.

The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data do not contain principles specifically related to PGHD, but principles related to personal data in general. Even so, it is evident that many of these principles, as they are defined, can be applicable to PGHD, such as concepts related to transparency, accountability, and accurate information. While the original guidelines were created in 1980, a second group (made up of experts in academics, the government, the tech

community, the business sector, privacy enforcement authorities, and civil society) was consulted to review the entirety of this data security framework and make revisions (20). With little information about the stakeholder group, it is difficult to determine how much of a role 'civil society' – or ordinary citizens had in the development of these principles. Like the EU, Canada's legislature governing personal data, the Personal Information Protection and Electronic Documents Act (PIPEDA) was based on principles referred to as the "fair information principles" (Appendix D) (25). Again, while not directly about PGHD, these principles relate to the "collection, use, and disclosure of personal information" (25) and include concepts related to transparency, accountability, and access to information – much like the OCED principles. The Canadian Standards Association (CSA) originally created the fair information principles in 1996, as part of their Model Code for the Protection of Personal Information. Interestingly enough, this model code was based on the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (26, 27) mentioned above, which may explain the similarity between the principles in these two documents. The CSA's Model Code for the Protection of Personal Information was developed by a committee, which included stakeholders from businesses, the government, consumers, security experts, academics, and technology experts (27). Much like with the OECD principles, it is hard to determine how big of a role consumers played in the 45-person committee (27) that developed these principles.

In 2017, the American Medical Informatics Association (AMIA) created guiding principles and a policy framework based on redefining patient health to include a more patient-centred focus (28). Again, while not directly related to PGHD, the AMIA created what they called 'guiding principles' to consider when development data infrastructure (28). AMIA wished to incorporate a patient lens in order to use data for more patient-centred care. A stakeholder group, whose members were affiliated with various universities and healthcare entities, developed this document. These stakeholders specifically include health care providers, researchers, scientists, and patients. Specifically, "patient and consumer views" from three individuals were mentioned (28). This document include the 'guiding principles' which are the general principles, but interestingly also include 'policy principles' – which is specifically intended to help develop or refine legislature and regulations that chooses to follow these principles (Appendix E). Like the OECD principles, the ones created by AMIA emphasize transparency and access to data, but also adds elements of diversity and patient/caregiver partnership as core principles. Furthermore, these principles did seem to be developed with patient/consumer input (though the ratio of patient input compared to other stakeholders seems minimal) and a clear patient focus was evident in the principles.

In 2015, the Consumer Electronics Association (an association representing various consumer technology industries in the U.S) created "Guiding Principles on the Privacy and Security of Personal Wellness Data" (29). Like the above two examples, these aren't principles necessarily related to PGHD, but rather, are 'design principles' (Appendix F) to be considered when developing products that use PGHD (1, 29). Again, like the OECD and AMIA principles, the CEA focuses on issues related to transparency and accurate data, but additionally includes principles related protection from discrimination (29). The ONC, in particular, recommends that developers use these principles when designing their technology, and that relevant bodies continue to build on this work (1) (perhaps by introducing some components into legislature that affects PGHD collection, storage, and sharing). The CEA emphasizes that their principles are merely recommendations and are not meant to replace legislature such as HIPAA (29). A working group created the CEA's principles, though its exact membership is unclear.

Conclusion

Ultimately, it appears that while principles *related* to PGHD exist, there are no specific ones that are directly about PGHD itself. Principles that currently exist relate to personal data, design elements for technology using PGHD, and policy translatable guidelines related to the development of data infrastructure. Such principles, while not directly about PGHD, can still strengthen its cause and add legitimacy to the rising importance of using patient-generated health data. The principles described above have their own unique characteristics to them, including elements of diversity and partnership with patients. The latter is especially important. Since we are dealing with *patient*-generated health data, it is a necessity that they are involved in the process, in whatever capacity they can and want to be involved. On that note, many of these principles were designed with the help of some sort of expert, working, or stakeholder group, often including patient and consumer involvement. The extent of patient involvement in these groups cannot be know, but it is certainly a step in the right direction. There is a focus on these principles advocating for a patient-centred approach, especially advocating for patients' ability to access their information and transparency in data processes so patients are aware of what is being done with their data. However, rather than a group that includes patient or consumer views or a group that consult patients, it would be interesting to see a process work the other way around – that is, principles designed predominantly by patients for patients – with consultations with other stakeholders on an as needed basis. Although principles are available related to personal data and other PGHD-adjacent concepts, it would be interesting to produce principles directly focused on patient-generated health data. Principles could also be built upon to create frameworks, or act as guidelines for policymakers and developers to take into consideration when creating legislature or designing technology.

It is not uncommon for policymakers to consider principles when designing legislature. The EU GDPR and Canada's PIPEDA are good examples of such legislatures. In some countries, like the U.S and Canada, while current laws exist to protect personal health information, such legislature was created before the popular use of technology to self-collect health data. As these technologies are now being used to collect, store, and facilitate the exchange of PGHD, it is important for legislature to remain up to date and current, reflecting the changes that have been brought forward by technology. While the scope of this paper focused on protecting PGHD by ensuring proper confidentiality and security measures, it is important to note that patients have concerns and wishes that fall outside the scope of security, many of which were discussed in the previous paper. As such, it is imperative that any principles (and work built off of them) reflect all the wishes of patients, even outside the scope of security. Patients should not only have the ability to access their data, but should also be able to add to or change their information and have those changes reflected on all platforms, they should have a clear decision as to who has their information and what is being done with it, and should be able to revoke access if desired. Patient's identifying information should be safeguarded and all precautions should be taken to ensure they face no discrimination that may result in loss in career advancements, job opportunities, or medical support. To truly understand what patients desire and how to best achieve these goals, it's important to partner with patients, to consult them, and let them take the lead in deciding what their rights should be. Lastly, if new legislature is to be created, or current legislatures are to be amended, it strongly advised that consultations with various stakeholders are undertaken. If such legislature were to affect not only patients but also healthcare providers, researchers, and technology developers – it would be prudent to tackle their concerns from the outset and have them reflected in the new legislation to strengthen them and minimize any gaps.

References

1. The Office of National Coordinator for Health Information Technology. Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research through 2024 [Internet] Washington, DC; 2018 [cited 2019 August 7]. Available from https://www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.
2. Information and Privacy Commissioner of Ontario. A Guide to the Personal Health Information Protection Act [Internet]. Toronto; 2004. [cited 2019 August 7]. Available from https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf.
3. Atkinson K, Bell C, Wilson K. So you want to build a health app, eh? Cmaj BLOGS. [Internet]. 2018. [cited 2019 August 7]. Available from https://cmajblogs.com/so-you-want-to-build-a-health-app-eh.
4. Government of Canada. Personal Information Protection and Electronic Documents Act [Internet] Ottawa; 2000. [cited 2019 August 7]. Available from https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html.
5. Grindrod K, Boersema J, Waked K, Smith V, Yang J, Gebotys C. Locking it down: The privacy and security of mobile medication apps. Can Pharm J (Ott). [Internet] 2016 [cited 2019 August 7];150(1):60–66. doi:10.1177/1715163516680226. Available from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5330422/
6. Government of Ontario. Personal Health Information Protection Act [Internet] Ontario; 2004. [cited 2019 August 7]. Available from https://www.ontario.ca/laws/statute/04p03.
7. Government of Ontario. Personal Health Information Protection Act, 2004: An Overview. [Internet] Ontario; 2004. [cited 2019 August 7]. Available from http://www.health.gov.on.ca/english/providers/project/priv_legislation/overview_leg.pdf.
8. U.S Department of Health and Human Services Office for Civil Rights. HIPAA Administrative Simplification. [Internet]. Washington, DC; 2013. [cited 2019 August 7]. Available from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
9. Juliana De Groot. What is HIPAA compliance? 2019 HIPAA Requirements 2019. *Digital Guardian.* https://digitalguardian.com/blog/what-hipaa-compliance.
10. Shailendra Sinhasane. What is PHI and What is Not PHI? 2018. *Mobisoft*. https://mobisoftinfotech.com/resources/blog/what-is-phi-and-what-is-not-phi/.
11. Rouse M, Wallask S, DelVecchio A. protected health information or (PHI) or personal health information. ScearchHealthIt. [Internet]. c2019. [cited 2019 August 7]. Available from https://searchhealthit.techtarget.com/definition/personal-health-information.
12. U.S Department of Health and Human Services Office for Civil Rights. Health App Use Scenarios & HIPAA [Internet] Washington, DC; 2016. [cited 2019 August 7]. Available from https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf
13. Primeau D. Is Patient Generated Health Data the Future of Healthcare? Primeau Consulting Group. [Internet]. 2018. [cited 2019 August 7]. Available from https://primeauconsultinggroup.com/is-patient-generated-health-data-the-future-of-healthcare/
14. Robeznieks A. Why patients worry about cybersecurity and patient-generated data. American Medical Association. [Internet] 2019. [cited 2019 August 7]. Available from https://www.ama-assn.org/practice-management/digital/why-patients-worry-about-cybersecurity-and-patient-generated-data.

15. U.S Department of Health and Human Services Office for Civil Rights. Can HIPAA address patient generated data? [Internet]. Washington, DC; 2015. [cited 2019 August 7]. Available from https://hipaaqsportal.hhs.gov/a/pages/answered-questions.
16. Brook C. Handing Patient-Generated Health Data Security. Digital Guardian Blog. [Internet]. 2018. [cited 2019 August 7]. Available from https://digitalguardian.com/blog/handling-patient-generated-health-data-securely.
17. Nøhr C, Parv L, Kink P, et al. Nationwide citizen access to their health data: analysing and comparing experiences in Denmark, Estonia and Australia. *BMC Health Serv Res*. 2017 [cited 2019 August 7];17(1):534.. doi:10.1186/s12913-017-2482-y. Available from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5547535/
18. Official Journal for the European Union. General Data Protection Regulation GDPR. [Internet]. European Union; 2016. [cited 2019 August 7]. Available from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
19. EU GDPR Protal. How did we get here? [Internet]. [date unknown] [cited 2019 August 7]. Available from https://eugdpr.org/the-process/how-did-we-get-here/.
20. The Organisation for Economic Co-operation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. [Internet]. Paris; 2013. [cited 2019 August 7]. Available from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
21. Understanding Patient Data. An Introduction to the GDPR – and what it means for patient data. [Internet] United Kingdom; 2018. [cited 2019 August 7]. Available from https://understandingpatientdata.org.uk/news/gdpr-and-patient-data
22. Bhatia P. Data subject rights according to GDPR. Advisera. [Internet]. 2010. [cited 2019 August 7]. Available from https://advisera.com/eugdpracademy/knowledgebase/8-data-subject-rights-according-to-gdpr/.
23. Information and Privacy Commissioner of Ontario. Your Health Privacy rights in Ontario. [Internet]. Toronto; [date unknown]. [cited 2019 August 7]. Available from https://www.ipc.on.ca/health/your-health-privacy-rights-in-ontario/.
24. Finnegan G. New EU rules aim to boost protection of patient data. But is healthcare ready? Science business. [Internet]. 20158. [cited 2019 August 7]. Available from https://sciencebusiness.net/healthy-measures/news/new-eu-rules-aim-boost-protection-patient-data-healthcare-ready.
25. Office of the Privacy Commissioner of Canada. PIPEDA fair information principles. [Internet]. Toronto; 2019. [cited 2019 August 7]. Available from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.
26. CIPP Guide. CSA Model Code [Internet]. [place unknown]; 2010. [cited 2019 August 7]. Available from https://www.cippguide.org/2010/06/29/csa-model-code/.
27. PrivacySense. The 10 Privacy Principles of PIPEDA. [Internet]. [place unknown]; 2015. [cited 2019 August 7]. Available from http://www.privacysense.net/10-privacy-principles-of-pipeda/.
28. American Medical Informatics Association. Redefining our Picture of Health: Towards a Person-Centered Integrated Care, Research, Wellness, and Community Ecosystem. [Internet]. Maryland; 2017. [cited 2019 August 7]. Available from https://www.amia.org/sites/default/files/API-2017-White-Paper-Redefining-our-Picture-of-Health.pdf/
29. Consumer Electronics Association. Guiding Principles on the Privacy and Security of Personal Wellness Data. [Internet]. Virginia; 2015. [cited 2019 August 7]. Available from https://fpf.org/wp-

content/uploads/2015/10/CEA-Guiding-Principles-on-the-Privacy-and-Security-of-Personal-Wellness-Data-102215.pdf.

Appendix A – the OECD's Eight Principles for the Processing of Personal Data (used by the GDPR)

Collection Limitation Principle

There should be limits to the collection of personal data, data should be obtained by lawful and fair means, and where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purpose for the collection of data should be specified at the time of collection and data should not be used for anything other than its original intention without again notifying the data subject.

Use Limitation Principle

Personal data should not be used for purposes outside of the original intended and specified purpose, except with the consent of the data subject or the authority of the law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Individuals should have easy access to information about their personal data, who is holding it, and what they are using it for.

Individual Participation Principle

An individual should have the right to know if a controller has data about him/her and to have access to that data in an intelligible form for a charge, if any, that is not excessive. An individual should also have the right to challenge a controller for refusing to grant access to his/her data, as well as challenging the accuracy of the data. Should such data be found to be inaccurate, the data should be erased or rectified.

Accountability Principle

Data controllers should be accountable for complying with the measures detailed above.

These guidelines were the basis of many national laws regarding data privacy, however, they were non-binding and the levels of data protection varied greatly even amongst different EU member states.

Appendix B – GDPR's Data Rights

Right to information

This right provides the data subject with the ability to ask a company for information about what personal data (about him or her) is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom his or her personal data is shared.

Right to access

This right provides the data subject with the ability to get access to his or her personal data that is being processed. This request provides the right for data subjects to see or view their own personal data, as well as to request copies of the personal data.

Right to rectification

This right provides the data subject with the ability to ask for modifications to his or her personal data in case the data subject believes that this personal data is not up to date or accurate.

Right to withdraw consent

This right provides the data subject with the ability to withdraw a previously given consent for processing of their personal data for a purpose. The request would then require the company to stop the processing of the personal data that was based on the consent provided earlier.

Right to object

This right provides the data subject with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent, if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that his or her personal data should not be processed for certain purposes while a legal dispute is ongoing in court.

Right to object to automated processing

This right provides the data subject with the ability to object to a decision based on automated processing. Using this right, a customer may ask for his or her request (for instance, a loan request) to be reviewed manually, because he or she believes that automated processing of his or her loan may not consider the unique situation of the customer.

Right to be forgotten

Also known as right to erasure, this right provides the data subject with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right, and depends on your retention schedule and retention period in line with other applicable laws.

Right for data portability

This right provides the data subject with the ability to ask for transfer of his or her personal data. As part of such request, the data subject may ask for his or her personal data to be provided back (to him or her) or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Appendix C – Ontario's PHIPA Rights

PHIPA gives you the right to:

- be informed of the reasons for the collection, use and disclosure of your personal health information;
- be notified of the theft or loss or of the unauthorized use or disclosure of your personal health information;
- refuse or give consent to the collection, use or disclosure of your personal health information, except in certain circumstances;
- withdraw your consent by providing notice;
- expressly instruct that your personal health information not be used or disclosed for health care purposes without your consent;
- access a copy of your personal health information, except in limited circumstances;
- request corrections be made to your health records;
- complain to our office if you are refused access to your personal health information;
- complain to our office if you are refused a correction request;
- complain to our office about a privacy breach or potential breach; and
- begin a proceeding in court for damages for actual harm suffered after an order has been issued or a person has been convicted of an offence under *PHIPA*.

Appendix D – PIPEDA Fair Information Principles

Accountability

An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Identifying Purposes

The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Limiting Collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Limiting Use, Disclosure, and Retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Accuracy

Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

Openness

An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Individual Access

Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Challenging Compliance

An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

Appendix E – AMIA Guiding Principles

	Guiding Principle	Policy Principle
Partnership	Patients, care givers, and research participants are integral partners in the development of digitally supported health.	Public policies and programs that are meant to support and encourage (trusted and safe) digitally supported health should include patients, care givers, and research participants as integral partners.
Individual Control	Individuals have rights to access and use data collected by technologies that support their health.	Public policy should make data open, available, and controllable by those from whom the data derive.
Transparency	Individuals deserve transparency in how their data are used and re-used by technologies that support their health.	Public policy should incentivize transparency, openness, and consistency among data source terms and conditions – for use and reuse – within and outside the current purview of HIPAA (e.g., wearables, medical devices, remote monitoring sensors, mobile apps, websites including social media, patient portals, health information exchanges, and EHRs).
Data as a Social Good	Decisions related to data access and data sharing are fundamental expressions of social and ethical norms in a modern, connected society.	Public policy should encourage socially responsible and ethically consistent data access and data sharing that enable the n-of-1 to improve the health of the n-of-many, and the n-of-many to inform the treatment of the n-of-1.
Diversity	Special emphasis should be applied so that all populations can participate in, access, and benefit from advances in technologies that support health.	Public policy must ensure that diverse and underserved people and populations are able to participate in, access, and benefit from advances made in digital health across ability, culture, health literacy, and socioeconomic status.

Appendix F - CEA's Guiding Principles on the Privacy and Security of Personal Wellness Data

Security

Robust security measures are the foundation of good data management. While consumers have access to many tools that allow them to secure their data, companies must do their part to secure personal wellness data from the outset.

Policy and Practice

Consumers need to understand how personal wellness data is handled to be comfortable using health-related devices and services.

Concise Notice

Consumers may be unable to understand lengthy privacy policies, which would impede their ability to understand how personal wellness data is collected and used.

Unaffiliated Third Party Transfers

Consumers seek transparency about and sometimes want to control personal wellness data transfers among companies.

Fairness

Personal wellness data collected from Internet of Things devices, combined with new data analytics, can provide many consumer benefits. Analytics can help consumers learn more about their health, enable them to reach their goals, and produce socially useful outcomes. Companies need to guard against the possibility that data analytics unintentionally could create unjust or prejudicial outcomes for consumers. While CEA is not aware of any such outcomes, this principle, which is inspired by existing U.S. federal, anti-discrimination laws, guards against that possibility throughout the lifecycle of their products.

Personal Data Review, Correction, and Deletion

Consumers wish to manage personal wellness data carefully. The ability to review, correct, or delete personal wellness data permits consumers to guard against inaccuracies or dissemination of the data beyond their control.

Advertising Communications

Advertising is a useful tool that facilitates communication between companies and consumers. However, consumers want to control how personal wellness data is used for that communication.

Law Enforcement Response

Consumers and companies alike are concerned about government access to personal wellness data. While companies must comply with legal process, they can be transparent with consumers about when and how they respond to lawful requests for data.