The Future of Privacy Forum @ RightsCon 2020

Exploring Blurred Expectations of Health Data Privacy Across the Patient-Consumer Spectrum

... and what comes next?

Healthcare is rapidly transitioning from a periodic activity in fixed, traditional health care settings to an around-the-clock activity that involves the generation, use, and integration of data reflecting many aspects of individuals' lives and behaviors (e.g., activity monitors, sleep quality sensors, smart toothbrushes, Bluetooth enabled hearing aids, connected medical devices, etc.).

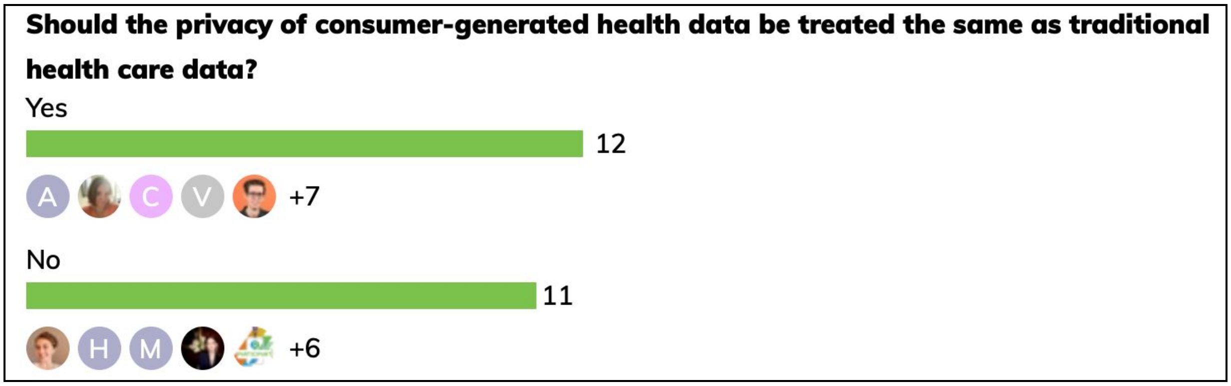
Unsurprisingly, individual experience with and expectations of health data privacy may vary or become blurred across these rapidly expanding contexts. This risk is particularly acute when health data is collected using the same kinds of modern technologies in both traditional health and "recreational" contexts (e.g., wearables, health apps, direct-to-consumer genetic testing, etc.). These phenomena, along with a growing dependence on big data sets involving the combination of health data from traditional and non-traditional health information platforms, have created a blurred line along a broadening patient-consumer spectrum. What results today are blurred expectations of health data privacy among multiple stakeholders and a growing number of companies that want to: 1) differentiate themselves from companies who do not publicly prioritize consumer health data privacy; and 2) establish best practices and standards for organizations that interact with consumers in both clinical and recreational contexts.

On July 27, 2020, during the RightsCon 2020 virtual conference, the Future of Privacy Forum's (FPF's) Health Policy Counsel and Lead, Dr. Rachele Hendricks-Sturrup sat down with three health data governance and policy experts to explore the privacy and policy implications across this broadening spectrum in a panel entitled, "Frontiers in health data privacy: navigating blurred expectations across the patient-consumer spectrum:"

- **Carolina Rossini**, Co-Founder and CEO, Portulans Institute
- **Megan Doerr**, Principal Scientist - Governance, Sage Bionetworks
- **Teresa Patraquim da Conceição,** Head Privacy Team - International, Novartis

Privacy in Consumer-Generated Versus Traditional Health Care Data

Dr. Hendricks-Sturrup and the panelists discussed a range of issues on this topic, beginning with the unequal or unbalanced distribution of risks and benefits to data sharing across healthcare and health consumer contexts. During the panel, a poll was taken to garner the panel audience's perspectives regarding the privacy of consumer-generated versus traditional health care data. Just over half (52%) of the audience members who participated in the poll felt that the privacy of consumer-generated health data *should* be treated the same as traditional health care data:


Should the privacy of consumer-generated health data be treated the same as traditional health care data?

This rather split poll result holds two key messages for policy makers:

1) It suggests that broader survey engagement on this topic is warranted to inform all levels of policy; and
2) It offers a visual example of how the privacy expectations of individuals across the patient-consumer spectrum have become blurred.

Clearly, dialogue is needed to inspire the development or evolution of company best privacy practices across the patient-consumer spectrum. The panelists took on this challenge and ended with core topics to consider as stakeholders take next steps to grapple with privacy expectations across the broadening patient-consumer spectrum.

Data Availability Engenders Discovery and Collaboration… at a Price

Data sharing accelerates biomedical discovery, creates opportunities for greater research yield, and contributes to the process of solidifying scientific consensus. Open data systems, especially, yield competitive value, as researchers aim to minimize the transaction cost of acquiring useful data, while also respecting the privacy wishes of data subjects. Some researchers might aspire toward the creation and use of a centralized, interoperable big data repository that houses electronic health record and insurance claims data combined with consumer-generated health data. However, given the patchwork of international data protection and privacy regulations, federated data queries will likely be the way forward.

Robust local, regional, and national datasets and repositories hold promise to help researchers better understand disease onset and progression, and ultimately use that data to model or formulate interventions that might improve health care services and lower health care expenditures. As these data sets are aggregated, data controllers should attend not only to data quality and other standard metrics of usability, but also, as Mangravite and Wilbanks highlighted in a recent perspective on data management and sharing, their **availability** and **freedoms.** In their framework, availability refers to the size of the population to whom a specific data set is available. While freedoms describe the constraints under which a data user must work. As a general rule, data that are transient pose lower risk to privacy than data that rarely or never change. For this reason, step counts may understandably have different availability and freedoms for use than genomic data.

Applying the framework of availability and freedoms to traditional health data and non-traditional health data highlights the spectrum of privacy concerns posed by big data research. Regulators and data experts should consider the availability-freedom axis not only for traditional health data, but also for "non-traditional" health data. Robust community engagement is needed to identify community expectations and to establish local norms for data availability and freedoms.

Context is Critical

Individuals may be motivated to share private data broadly if they feel it can help a loved one, as in the case of rare disease research. By contrast, others may "consent" under false pretenses or duress to the use of their data. The context under which data is collected is critical to determining how those data can be meaningfully used.

Smart Regulation is Key to Protection

It is important to note that there is no failsafe technical mechanism that guarantees privacy or anonymity. As technologies to protect data advance, so too do technologies used by attackers to breach or misuse data. Yet troves of private data, both traditional and non-traditional, are needed to solve our biggest health challenges. Thus, regulations must protect people from stigmatic or discriminatory use of their data.

The traditional health data environment is highly regulated, in terms of confidentiality, privacy, and protections offered. However, the same is not true for consumer-related health data. The panelists argued that rather than forcing the public to adapt individuals' expectations driven by context clues or data type, the same safeguards and accountability must be implemented for consumer-related health data. As regulations develop, it is essential to consider that consumers are especially vulnerable. The political context of a country, including national and local governance, can pose obstacles to developing efficient, consistent regulation. However, a **social contract** ought to incorporate supportive regulation to ensure that data may be shared for innovation, research, growth, but also respect the human right to privacy.

A range of privacy regulatory frameworks have been developed worldwide and different foundational cultures across the globe yield varying expectations of what privacy regulation should look like. For instance, the GDPR outlines comprehensive privacy protections for consumer health data, but this level of protection contrasts that several other countries like the U.S. and Brazil until recently (Brazil approved in August 2018 a general personal data law, which will apply soon). Particularly, in the U.S., a comprehensive privacy law or protection standard is absent or exists only minimally at the state level, despite its thriving culture of technological and data innovation.

Informed Consent Remains Important

Data collectors must make sure their standard informed consent process is comprehensible, accessible, and appropriate for the intended audience. Information conveyed during the informed consent process should be based on important questions that include but are not limited to the following: "What are their rights?," "What happens to their data?," "What are the long-term

consequences of sharing their data?" Accessible and clear informed consent tools are key to making informed health decisions across recreational and traditional health settings.
This is especially important because the overarching intent and purpose of informed consent can easily become compromised in consumer settings that may require or prefer scaled or perhaps broad consent. Therefore, the challenge ahead rests in determining not just if but also how informed consent can become meaningful for data subjects in both traditional and non-traditional health settings.

Providing information to individuals is key, but it is worthwhile to note that in the traditional health setting, other legal bases than consent may apply. The European Data Protection Board opinion concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)[1] is an example of adequate legal basis other than consent.

Trust in Data Use Requires Transparency and Governance

Researcher credentialing poses a challenge, especially when systems of trust must be transparent and do not rely solely on affiliation with known institutions in order to incorporate a more inclusive solving pool. Health data governance models consider key stakeholders or actors in the data exchange process, paying close attention to "who" is involved and "how" and "why" the data-driven service is being offered, in order to elicit an appropriate governance response. Poorly informed machine learning tools and unintentionally mis-aligned algorithms can perpetuate discrimination in a range of contexts, especially in healthcare systems, undermining patient-consumer trust. By consistently and carefully considering how data is used and by remaining intentional in terms of fairness and equity, trust can be established.

Data Subject Representation, Rights, and Respect are Paramount

It is important to consider both physical and digital barriers to tackle in order to avoid the marginalization of individuals, improve data accuracy, and increase the representativeness of the data. Many human rights intersect and conflict each other in this field, such as access to health, privacy, and even economic development. In order to ensure that the data are truly representative, organizations must work to include solvers who come from the subject communities. The lack of *accurate* and *representative* data from marginalized populations will impact research and the health of those populations in the longer term.

Regulation must protect individuals from discrimination: if people share data for the betterment of humanity, they should not be at risk of discriminatory harms. Jasmine McNealy's ecology model of data reflects an important intersection with the consideration that individual data yields implications on others. Essentially, individual-only models of data governance, such as models that rely solely on individual consent or "ownership" of data, are not sufficient. Specifically, protections for data that carries risk of social stigma, such that it can be used to deny or limit any rights or benefits of individuals or populations, are more valuable.

[1] Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b), Adopted on January 23, 2019.

Data Justice Means Addressing the Digital Divide

Data must be collected from all areas of society to combat the digital divide, as only representative data will help make a difference. Diversity and inclusion are crucial during the whole cycle (i.e. knowing what data should be collected, who collects the data, and to whom the data is transferred). Digital inclusion is a paramount first step to include data justice in the long term. From a policy perspective, addressing the digital divide to reduce inequality should be a government priority. Implementing an education-based approach, such as imparting critical thinking about the information and data the individual provides and receives, would serve to reduce the digital divide.

It is imperative to uphold data justice. If data is not representative, and if the problem-solvers are not representative, subsequent actions not only do a disservice, but evaluators also miss out on valuable insights.

What's Next?

These core topics can be used to set a collaborative agenda to advance discussions and promote discourse around contemporary expectations and experiences in health data privacy across the patient-consumer spectrum. To successfully navigate blurred expectations of privacy across this spectrum and make progress toward establishing meaningful legal and policy frameworks and best practices, diverse stakeholders from industry, academia, and civil society must be engaged and barriers to their collaboration must be addressed.

The FPF Health Initiative is committed to developing and disseminating best privacy practices that can guide policymakers, civil society, scholars, and industry stakeholders. To learn more about this initiative, contact Dr. Rachele Hendricks-Sturrup at rhendrickssturrup@fpf.org.

Recommended Readings & Recordings

- View Megan Doerr's TEDx Talk entitled, "Have You Given Away Your Medical Privacy?," where she discusses how tricky it can be to keep your data private and also the importance of safely sharing your health data with scientists.
- Given the panelists' discussion about the work of Dr. Jasmine McNealy, listen to the Data & Society Databite No. 127 entitled "An Ecological Approach to Data Governance," by Dr. McNealy, moderated by Sareeta Amrute.
- Given the growing need for a common taxonomy or naming convention for health data across the patient-consumer spectrum, and example best privacy practices across this spectrum, read the FPF white papers entitled "A Taxonomy of Definitions for the Health Data Ecosystem," released in May 2019, and "Privacy Best Practices for Consumer Genetic Testing Services," released in July 2018.
- Regarding direct-to-consumer genetic testing companies' increasing engagement in the health and pharmaceutical spaces and the endorsement of FPF's Privacy Best Practices for Consumer Genetic Testing Services, by certain members of the clinical community, read the National Academies' 2019 public workshop proceedings entitled, "Exploring the Current Landscape of Consumer Genomics: A Workshop".
- Read relevant proceedings from another National Academies 2009 workshop entitled, "Health Literacy, eHealth, and Communication: Putting the Consumer First: A Workshop."