August 21, 2020

Federal Trade Commission
Office of the Secretary
Constitution Center
400 7th St., SW, 5th Floor, Suite 5610
Washington, D.C. 20024

Re: Federal Trade Commission Workshop, "Data to Go: An FTC Workshop on Data Portability"

Dear FTC Representative:

The Confidentiality Coalition appreciates the opportunity to submit comments on data portability and, specifically, the benefits and challenges of data portability, for purposes of the Federal Trade Commission (FTC) Workshop, "Data to Go: An FTC Workshop on Data Portability."

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective confidentiality protections for health care consumers. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and health care consumers while, at the same time, enabling the essential flow of information that is critical to the timely and effective delivery of health care, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

The FTC seeks input on a range of questions raised by data portability, such as the potential benefits to consumers of data portability as well as the potential risks to consumer privacy and how those risks might be mitigated, including how best to ensure the security of personal data that is being transmitted from one business to another.

General Comments

Before addressing the FTC's specific questions, the Confidentiality Coalition would like to state its strong support for efforts to improve consumer access to their own health records, which is essential to allow consumers to better manage their care and make decisions about it. We also strongly support efforts to improve data exchange and

interoperability between health care organizations, which is essential for care coordination, more efficient delivery of care and improved health outcomes.

A key consideration in data portability of health records is to ensure that there are comparable privacy and security protections for information shared with entities subject to the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and those that are considered non-HIPAA covered entities. The need for such a comparable regulatory regime to protect health records in the hands of non-HIPAA entities has become more urgent and highlighted by the issuance in May 2020 of the ONC 21st Century Cures Act final rule by the Department of Health and Human Services' (HHS) Office of the National Coordinator for Health Information Technology (ONC) and the Interoperability and Patient Access final rule by the Centers for Medicare and Medicaid Services (CMS). These Rules seek to improve interoperability and health data portability and allow health data to flow not only between HIPAA entities, but also from HIPAA entities to non-HIPAA entities, such as third-party apps. However, HHS does not have the regulatory authority to require that these non-HIPAA entities comply with the privacy and security provisions of the HIPAA Privacy and Security Rules. The CMS and ONC Rules will result in large gaps in privacy and security protections for these non-HIPAA covered entities, with many more health records falling outside of the strong protections of HIPAA, oftentimes without consumers understanding this or appreciating its implications.

It is important not only that health information held by non-HIPAA entities be subject to robust privacy and security protections comparable to HIPAA, but also that the regulatory regime governing these records harmonize with HIPAA so as to avoid conflicting regulatory approaches imposing barriers to the appropriate flow of health information and on consumers' privacy protections. As became apparent during the opioid crisis, the lack of alignment between the rules governing substance use disorder records (42 CFR Part 2 records) and HIPAA resulted in barriers to care or lack of care coordination for many patients who needed it the most. It is only with the passage of the CARES Act in March 2020 that HHS has been charged with issuing regulations to bring 42 CFR Part 2 in much closer alignment with HIPAA, which will benefit patients and the health care system as a whole.

Finally, the success of health information data portability will depend on the implementation of uniform national standards similar to those required by HIPAA for HIPAA-covered transactions. Currently, health care organizations are facing an increasingly complex web of different state laws and standards governing data portability, including conflicting, formats, specifications and requirements. This complexity increases the cost of compliance at a time when health care organizations are dealing with unprecedented demands on their resources as a result of the COVID-19 pandemic. Furthermore, these conflicting standards create significant barriers to portability, rather than facilitating it, to the detriment of health care consumers.

Specific Comments

Below are our comments on some of the specific questions asked by the FTC.

1. Benefits and Costs of Portability, Including Through Regulation

[What have been the benefits and costs of data portability? What are the benefits and costs of achieving data portability through regulation?]

There are significant benefits to health care consumers and the health care system from improved portability of health care records. As CMS and ONC have stated, data portability allows patients to be in control of their own health care and make informed decisions based on having a better understanding of the care they have received as well as the costs of that care. It will also give the patient's health care providers a more complete record of the patient's care, which will improve health care decisions and result in better care coordination and management.

There are both operational and compliance costs to be considered in achieving data portability. However, there is an even larger cost of reduced protection being afforded to health information that is shared with entities that are not required by *any* law to protect those records. This latter cost can and should be avoided by regulation that provides comparable protections to those provided by HIPAA for health care information held by non-HIPAA entities. Operational and compliance costs would be significantly reduced, and unnecessary hurdles to health information portability removed, for health care organizations if they are subject to a single national standard and regulatory framework for data portability, rather than multiple inconsistent and potentially conflicting state standards.

2. Data Security

[Who should be responsible for the security of personal data in transit between businesses? Should there be data security standards for transmitting personal data between businesses? Who should develop these standards?]

It is imperative that data portability not come at the expense of data security, particularly in the case of sensitive records, such as health records. Data security should be the responsibility of all parties involved in the data transmission, including the party transmitting the data as well as the party receiving or accessing the data, in each case to the extent of their control over the data. Minimum data security standards are essential for health care records, and the assurance of rigorous data safeguards underpins the sharing of health care records by and between HIPAA entities. Similar risk-based security standards should be required of non-HIPAA entities. In addition to HIPAA, there are other comprehensive and well-tested security standards, such as the NIST security standards, that can be used by regulators to form the basis for minimum security standards required of all entities that process, transmit or store health care data for consumers.

3. Identity Verification

[How do companies verify the identity of the requesting consumer before transmitting their information to another company?]

While health care organizations and financial institutions have long had to manage verifying with certainty the identity of individuals requesting access to their own information, the challenges have only grown in recent years as more personal information is available online and more individuals seek to allow other entities to request access to their information on their behalf. In particular, hospitals and other health care providers grapple with the difficulties of confirming not only the identity, but also the authority, of third parties requesting access to patient information purportedly at the direction of patients. An important first step that would help health care organizations in this regard is to improve data matching algorithms and standardize data elements to improve the accuracy of patient matching. The Confidentiality Coalition supports efforts to standardize patient demographic data, such as patient addresses by, for example, applying the U.S. Postal Service Standard to addresses. Research by the Pew Research Center in collaboration with Indiana University has shown that use of the U.S. Postal Service standard for addresses can increase match rates by approximately 2-3 percent—which would make a meaningful difference, allowing the matching of tens of thousands more records.[1] Standardizing last name alongside address showed further improvement in match rates (up to approximately 8 percent). It is for this reason that the Confidentiality Coalition also supports efforts to provide HHS funding for similar data matching efforts and solutions to improve unique patient identification. We recommend that the FTC support HHS' efforts in this regard for health care consumers. Finally, government regulators should exercise caution and avoid being overly prescriptive regarding the exact data elements or methodology required for verification, since this will vary based on the circumstances and data held. Instead, as with security standards, organizations should have flexibility in how they implement the standards, taking into account their scale, environment and risks.

4. Consumer Trust

[Are there research studies, surveys, or other information on the impact of data portability on consumer autonomy and trust?]

While not specifically about data portability, there are several recent surveys on contact tracing applications (apps) that are instructive on the issue of consumer trust

---

[1] See https://www.pewtrusts.org/en/research-and-analysis/articles/2019/08/08/wide-variety-of-groups-support-standardizing-addresses-in-electronic-health-records ("*Broad support for the use of the USPS standard follows the publication of research earlier this year from Indiana University that found this change could improve match rates by a small but important margin—enough to correctly match tens of thousands or more records each day. An organization with a match rate of 85 percent, for example, could see its unlinked records reduced by 20 percent with standardizing addresses alone. The research further revealed that standardizing last name in conjunction with address could improve match rates from approximately 81 percent to 91 percent, which would reduce the number of unmatched records by half.")* (accessed August 6, 2020).

and data portability. These surveys show that most U.S. consumers distrust contact tracing apps, in large part because of concern and confusion regarding the data they will collect, the purposes for which it will be used, and with whom and how it will be shared.[2] Even in surveys conducted by technology companies themselves that show growing acceptance of the benefits that such apps can offer, consumers overwhelmingly preferred apps provided by the federal or state government followed by those offered by local hospitals or health systems.[3] These surveys make clear that without consumer trust in the privacy and security protections of their health data, even the most sophisticated technological solutions to facilitate appropriate data sharing and portability will not succeed. Key components in building consumer trust are not only choice and control over the data to be shared, but more fundamentally, assurance that the data will be kept secure and protected from misuse. Such assurance can only be provided through a regulatory framework that requires and enforces a base line set of protections for the data and provides adequate privacy protections to health care data once it is no longer covered by HIPAA.

The Coalition appreciates the opportunity to provide comments on data portability and stands ready to work with the FTC and other stakeholders as it seeks to bring the many benefits of data portability to consumers while ensuring that their most sensitive records are appropriately used and protected. Please contact me at tgrande@hlc.org or at (202) 449-3433 if there are any comments or questions about the comments in this letter.

Sincerely,

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

---

[2] See https://www.computerweekly.com/news/252486058/Consistent-trust-gap-in-contact-tracing-apps-in-US-Europe, https://developer-tech.com/news/2020/apr/30/study-americans-dont-trust-contact-tracing-apps/ and https://spectrum.ieee.org/the-human-os/biomedical/devices/survey-finds-americans-skeptical-of-contact-tracing-apps (accessed August 4, 2020)

[3] See https://www.prnewswire.com/news-releases/new-survey-reveals-growing-acceptance-around-covid-19-contact-tracing-and-exposure-notification-apps-301083480.html (August 4, 2020)