David Young Law
Compliance Bulletin

August 2022

Data harmonization - a requirement for mobility rights and integrated records networks[1]

The drive to "digitization" in all spheres of the economy, as well as society more broadly, implies burgeoning databases containing personal information. These databases offer opportunities for providing services more efficiently as well as, potentially, enhancing individuals' access to their information. However, interoperability among databases, even if within a wider ecosystem such as health care, has been difficult to achieve, to the detriment of fully realizing such functionalities.

Integration of data systems has been a goal within the health care sector since the digitization of medical records. A single electronic health record for every individual is perceived as the ultimate objective, enabling providers and their patients alike to have readily accessible and up to date information regarding an individual's health and care status. The real world however is that this goal is likely far off if not unachievable, reflecting the difficulties in aligning the diverse entities and provider roles contributing data to the record. More realistic is a goal of aligning the systems within a care community as part of a "network" of health care and other providers who contribute data to a common database, accessible by all participants, or communicating among themselves through the medium of such database.

For such networks to operate successfully there must be harmonization of the data – both technical format alignment as well as institutional alignment. This means that participants in a data ecosystem not only speak the same language but also are governed by the same administrative rules regarding data processing and protection. Such harmonization provides data holders with the ability to "talk" to one another and exchange data in the same electronic language and in substantive content, in a coherent, confident manner that enhances the efficiency and effectiveness of the services being provided.

Data sharing in the commercial context – mobility rights

To date, data "sharing" and integration has been most significantly a focus in non-commercial contexts, particularly health care. However, with the advent of data "mobility" or "portability" rights under second-generation privacy laws such as Quebec's Bill 64 and the proposed federal *Consumer Privacy Protection Act*, the "sharing" of data between commercial entities is likely to become more common, with concomitant requirements for not only technical data alignment but also institutional data harmonization. In a word, "mobility" of data in a business context - analogous to data sharing in the

[1] A version of this article was originally published by The Lawyer's Daily (https://www.thelawyersdaily.ca/, part of LexisNexis Canada Inc.

health care sector - means that data transferred from one organization's system can be utilized within a receiving system in a confident, seamless manner.

To this end, learning from the health care sector may be instructive for the new commercial mobility idioms.

Key elements

What are the key elements of data harmonization? Clearly, alignment of technical specifications and the technical interoperability of databases are important. However, to achieve meaningful integration of systems, the "institutional" framework of a data ecosystem also must be in alignment – mutuality of processing standards, data quality, data protection rules and security standards - governing all participants in a data ecosystem. Furthermore, if the data includes personal information – such as health or financial data – privacy must be at the core of the design – addressing authorization to communicate and use, accuracy, access protocols, security, and breach response. Meaning, that there must be substantial uniformity of data quality, data security, data access and data accountability rules.

Electronic Health Records

Health records systems sharpen the issues - where harmonized data is critical to ensuring consistent, comprehensive and up to date information regarding a patient. Such information has a potentially critical role in timely, effective care, including in life-saving circumstances. Inaccurate, incomplete or inconsistent information provided in a care context could have impactful negative health consequences, as well as potential reputational impacts.

Stating it differently, integrated health care requires confidence between sender and receiver – so that data recipients know that the information they are receiving is permitted to be disclosed, will be accurate and up to date enabling appropriate diagnosis and treatment, and has been protected from unauthorized access. Furthermore, senders must have the confidence that their patients' information will be protected.

In sum, health data ecosystems, to achieve institutional harmonization, address privacy as a key requirement.

How can these principles inform the operational requirements for the newly, or soon to be, legislated idiom of data mobility in business and consumer contexts?

Data mobility – Fintech

The instance of the rapidly expanding consumer-directed finance or "fintech" industry demonstrates how a holistic approach to data harmonization can address integration among participants within a mobility network.[2]

However, in contrast to the health sector integration model which has evolved essentially "from the ground up", through contract frameworks, the data mobility ecosystems are likely to be executed through regulations under the privacy laws or, potentially, through industry standards. The difference may explain at least partly the unachieved goal of full system integration within the health care sector.

It is understood that the new legislative data mobility rules are intended firstly to address fintech. This industry offers digital financial management services in competition with established financial services providers but requires access to their customers' financial data in order to do so. A regulated framework for data mobility is perceived as a secure means to enable transfer of such data from one organization to another, with required mutuality of safeguards and privacy standards among participants. It is also suggested that data harmonization may improve the quality of the services provided.

Some commentators have noted that data mobility is not a key aspect of a privacy rules framework but is intended to address primarily competition and consumer protection interests.[3] However, like in the health care world, protection of sensitive personal information must underlie any system for sharing. This means institutional data harmonization, with privacy as a key requirement.

Conclusions

For integration of data systems to operate successfully there must be harmonization of the data – meaning both technical format alignment as well as institutional alignment. The result is that participants in a data ecosystem not only speak the same language but also are governed by the same administrative rules for data processing and protection.

These idioms have been inherent in the long sought-for integration of non-commercial databases such as in health care. With the advent of "mobility rights" under the second-generation privacy laws, it is likely that they will become mandatory standards within commercial data ecosystems in order to address sharing requirements in evolving applications such as fintech and telecommunications.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

[2] Another potential application may be the telecommunications industry where customer transfers between providers is not uncommon.
[3] See: Teresa Scassa, "Data Mobility (Portability) in Canada's Bill C-11", Blog, January 12, 2021.