Duke SANFORD | CYBER POLICY PROGRAM

Health Sector Innovation Through Data Sharing: The Role of Government

By Limor Shmerling Magazanik and Luke Schwartz
September 2023

Executive Summary:

- Enhanced data sharing and collaboration in the health sector foster innovation, improve outcomes, and facilitate evidence-based decision-making. It is imperative to prioritize privacy and security when accessing sensitive health data, with governments assuming a crucial role in creating policies that balance data access with privacy protection. The United States and Israel have taken differing approaches to achieve this end, including mandates, incentive-based programs, and entirely voluntary approaches.
- In the US, many federal agencies regulate health data sharing, while Israel's centralized public health system, managed by the Ministry of Health, facilitates effective health data research and innovation.
- US federal legislation like HITECH and the 21st Century Cures Act establish incentives and requirements for promoting data interoperability. There are also state-level initiatives.
- Israeli regulatory mandates have led healthcare providers to prioritize data utilization for research, efficiency improvement, and enhanced medical treatment, however, the health data ecosystem has historically been siloed between HMOs which has made coordinated care complicated.
- In Israel, access to quality nationwide health data for non-HMO researchers is made possible through using the Timna national platform. Israel has strong privacy protection laws and regulations governing the secondary use of health data for research and access by private sector entities, ensuring data security and confidentiality. The US has privacy laws, such as HIPAA, that are generally more limited in scope than Israeli privacy regulations.
- Both countries are gradually adapting Fast Healthcare Interoperability Resources (FHIR), an API designed to standardize and facilitate the exchange of health information, to ease data interoperability.

- Moving forward, the US has the opportunity to expand and streamline data access to researchers while ensuring privacy and security. While robust regulatory environments and frameworks like FHIR facilitate progress in health data sharing and innovation, they should be paired with comprehensive privacy legislation to ensure data sharing and use that prioritizes patient autonomy.
- Relatedly, Israel has proposed legislation that would increase patient autonomy through data portability, while enhancing the usefulness of health data for research and care.

Author: Limor Shmerling Magaznik is a visiting scholar with the Sanford Cyber Policy Program. Luke Schwartz was a researcher at Duke University's Technology Policy Lab.

Publication Note: The authors would like to thank Professor Campbell Tucker and Professor David Hoffman for their feedback on the report.

Introduction

Data sharing and collaboration and its analysis in the health sector are critical for driving innovation that may bring us medical breakthroughs, more precise and individually tailored medicine, better efficiency in healthcare, and improved patient outcomes. Access to a wide range of big data sources may provide government policymakers with better evidence to guide their decision-making, enable researchers to advance their medical capabilities, and allow healthcare providers to improve their success rates. It may also provide insight into solving previously non-cured ailments. However, granting access to troves of sensitive personal health data must come hand in hand with robust privacy and security safeguards. Additionally, providers and researchers face challenges in gaining access to large-scale population data sets that may considerably promote clinical advancement. Hence governments often play critical roles in providing policies that allow for access to health data with appropriate guardrails to maximize innovation through data sharing while maintaining a high standard of patient data privacy and security. Two countries that have taken different approaches to achieve this goal are the United States and Israel. This article explores the commonalities and differences between their approaches.

United States

The United States' healthcare system is a fascinating and often confounding subject, with its intricate web of regulations, providers, and mix of public and private insurance plans, making it one of the most complex in the world. The US healthcare system is in a constant state of flux, often shifting in response to the priorities of newly elected presidential administrations or Congress. With a population of over 330 million people, the US healthcare system is responsible for the wide health-related needs of a highly diverse population. The US employs a mixed healthcare system with over 90% of the 330 million people split between public and private health coverage (unfortunately, 8.3% are uninsured). As of 2021, 35.7% (or roughly 118 million people) had public healthcare coverage. Public healthcare coverage includes Medicaid, Medicare, and Veteran Affairs (VA) services, with the vast majority of public healthcare stemming from Medicaid and Medicare. Medicaid insures low-income individuals while Medicare insures those aged 65 and older as well as younger individuals with certain disabilities or chronic conditions.

To add to the complexity, many federal actors regulate different parts of the system. At the top of the regulatory hierarchy stands the Department of Health and Human Services (HHS). The HHS is responsible for supervising all health-related agencies within the executive branch. While the exact number depends on how you classify the agencies, at least a dozen agencies fall under HHS's jurisdiction. A few agencies are predominantly responsible for regulating the sharing and interoperability of health data.

- Centers for Disease Control and Prevention (CDC)

The CDC plays a crucial role in protecting public health and safety by controlling and preventing the spread of diseases, injuries, and disabilities. One of their main functions is to collect, analyze, and disseminate health-related data, working closely with patients, providers, payers, and other government organizations (both federally and locally) to facilitate data sharing and interoperability.

- Centers for Medicare and Medicaid Services (CMS)

Just as the name suggests, CMS oversees Medicare and Medicaid programs nationwide. CMS also establishes numerous national standards for the use of electronic health records (EHR) in order to meet the requirements of publicly funded insurance; these effects often spill over into providers that accept private insurance as well.

- Federal Trade Commission (FTC)

Falling outside the HHS's purview, the FTC has taken an expanded role in recent years in regulating the sharing of health data that falls outside the scope of existing US health privacy legislation.

- Office of Civil Rights (OCR)

The OCR is responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA) and its security and privacy protections, which play a critical role in dictating how health data is stored and shared.

- Office of the National Coordinator for Health Information Technology (ONC)

The ONC is responsible for developing and enforcing national policies and standards related to health information technology. As such, they dictate how healthcare providers collect and store information. A major aspect of health IT is data sharing and interoperability.

Federal agencies collaborate to promote a regulatory environment for health data that facilitates innovation while minimizing potential stifling effects. As these agencies have equal footing, there is no hierarchy in terms of enforcement or rulemaking authority among them. However, they have different roles which can limit coordination.

The agencies are not the sole determiners of health data sharing and interoperability regulation in the United States. Their rulemaking authority on these matters is often dictated by congressional legislation. Throughout the past 14 years, there have been significant changes in the norms, best practices, and regulations surrounding health data sharing in the publicly funded side of the US healthcare system. These changes are due to coordinated efforts between Congressional legislation and federal agencies to respond to the evolving needs of patients and the healthcare system.

While there are some mandates that shape the health data sharing regulatory environment, many of the regulatory schemes created by the agencies are rooted in incentives. Incentive structures dictate a large amount of the US federal government's approach to encouraging innovation in health data sharing.

The use of incentives to encourage modern approaches to data sharing in the health sector really began in 2009 when Congress passed the Health Information Technology For Economic and Clinical Health Act (HITECH), which had two main components, each overseen by a different federal agency. The first arm, overseen by the OCR, expanded the purview and enforcement of HIPAA, which included strengthening security and privacy protections and imposing tougher penalties for HIPAA violations. These changes were instrumental in raising the bar for data security which is critical for data sharing.

The second arm of HITECH promoted the adoption and meaningful use of EHRs. It achieved this by tasking the ONC with creating a Health IT Certification Program. The program ensures that certified health IT meets the "technological capability, functionality, and security requirements adopted by the HHS." The certification sets forth certification criteria to improve the uptake and innovation of EHRs. While the certification is voluntary for private providers, it is mandatory for providers who accept publicly-funded insurance. As a way to increase adoption of the certification, HITECH introduced the "Meaningful Use" program which allocated a major portion of HITECH's budget to pay providers for adopting certified EHRs and accepting publicly funded insurance. While Meaningful Use began as an incentive program, it eventually transitioned into penalties if its provisions were not followed. As a result, most patients today can log onto their patient portals and have full digital access to their health records, in part due to the monetary incentives for healthcare providers to become health IT certified.

The next major legislation impacting health data sharing and interoperability was the 21st Century Cures Act passed in 2016. The Cures Act Act was designed to accelerate discovery, development, and delivery in the health sector. Title IV of the Cures Act, titled "Delivery" amends and extends many of the key tenets of HITECH. These changes promoted the modernization of American healthcare information. The Cures Act introduced provisions to advance the use of health information technology, enhance patient access to information, and improve interoperability. It did this primarily through voluntary incentive-based initiatives, but there were some mandates as well.

The Cures Act demonstrated a strong commitment to ensuring patient access to health data, with one of the biggest steps being the prohibition of Information Blocking. This provision amended section 3001 of HITECH and is included in section 4004 of the Cures Act. It prevents healthcare providers and networks from engaging in practices that limit the exchange, access, or use of electronic health information (EHI). The ONC's 2020 Cures Act Final Rule included the Information Blocking Rule (IB Rule), which is part of a broader initiative to implement the Cures Act and provide patients with secure, unrestricted, and prompt access to their EHRs in the format of their choice. While the IB Rule has been in effect since April 2021, its penalties do not become effective until September 2023 with fines of up to $1 million per violation, thus giving health providers a window to become compliant. Although the IB Rule has effectively mandated greater patient access to data (and will become even more effective once penalties are on the table), it lacks effective and accessible mechanisms for patients to voluntarily share their EHI with researchers, limiting researchers' access to the larger datasets necessary to conduct meaningful clinical research. As such, there have been repeated calls from health data policy experts for federal guidance on IB Rule implementation for research.

Beyond direct amendments to HITECH in the Cures Act, HITECH established a strong foundation surrounding interoperability and health information exchange that many elements of the Cures Act are built upon. One example is the Trusted Exchange Framework and Common Agreement (TEFCA), as described in section 4003 of the Cures Act. TEFCA sets forth guidelines for interoperability across the country, merging infrastructure and governance models to enable secure, efficient, and practical sharing of healthcare data while incorporating fundamental principles for policies and practices that can facilitate exchange between health entities. One of its primary goals is minimizing the conditions necessary for data exchange to occur. A key feature of TEFCA is the creation of Qualified Health Information Networks (QHINs), which are entities that have met the requirements of TEFCA and are authorized to exchange health information with other QHINs. There is a strong incentive to adopt TEFCA and become a QHIN as doing so makes the healthcare entity part of a network of trusted players that share data in a secure and standardized manner. However, implementing TEFCA and applying to become a QHIN are optional across public and private payers. However, many think that utilizing TEFCA and becoming QHINs could become mandatory for CMS providers and payers sometime in the future. This would be a critical next step to easing data access and interoperability which could improve research initiatives in the public side of the US healthcare system.

Furthermore, as outlined in Section 4002 of the Cures Act, an essential component of the legislation's goal to enhance interoperability was identifying an application programming interface (API) to facilitate health data sharing nationwide. The API selected was HL7's Fast Healthcare Interoperability Resources (FHIR), a data sharing API designed to standardize and exchange health information. FHIR is widely recognized as the industry gold standard for data interoperability and serves as the "how" for how patients, providers, and researchers access and share health data. The ONC chose to incorporate FHIR into their Health IT Certification on December 31, 2022, but CMS went a different direction by mandating FHIR for all CMS-regulated payers and providers effective on July 1, 2021. A major component of the CMS's use of FHIR is the "Blue Button API" which allows Medicare beneficiaries to request, receive, and send health data (such as for research purposes). The FHIR mandate is still in its relatively early days, and most affected actors are still focused on general compliance. However, it is soon time to turn the page and look toward what could be next for FHIR usage. The FHIR mandate on public healthcare has the potential to improve data access for clinical research projects.

As a result of the mandate, there are several government-sponsored research databases and programs that use FHIR. Each of these has distinct access requirements based on the data type and intended purpose. Two of the largest research databases are the National Health and Nutrition Examination Survey (NHANES) and Medicare Claims Data. NHANES, run by the CDC, gathers general health information from a yearly nationally representative sample of 5,000 Americans. Patients must provide informed consent to participate in the survey. NHANES is a de-identified dataset accessible by anyone on the CDC's website. While potentially beneficial, the data loses some value for research since it is fully de-identified. Medicare Claims Data, managed by CMS, contains health information on all Medicare beneficiaries and is governed by HIPAA regulations. Patient consent is not necessary for their data to be included in the database. Researchers must submit proposals for access to the database and sign a data use agreement specifying how the data will be used, protected, and stored. Researchers then view data through CMS's Virtual Research Data Center (VRDC) which provides secure access to patient data. While this can be a very helpful database, it has two major drawbacks: 1) the data mostly comprises individuals 65 and older and 2) the dataset is predominately used for studying healthcare delivery and outcomes. The impact and use of the Medicare database in clinical-focused research and epidemiology are limited due to the lack of more detailed health data. Overall, the US has some decent databases, but both have drawbacks that prevent them from being used for clinical research. Navigating around publicly developed databases can be complicated, as levels of consent and the types of access differ widely by database.

While most of the burden falls on the federal government to facilitate data sharing in the health sector, some state governments also play a role. To illustrate how state governments are promoting data sharing, two examples are provided. The first is New Jersey's Integrated Population Health Data Project (iPHD). Funded by the New Jersey Department of Health and operated by the Rutgers Center for State Health Policy, the iPHD collects population health data on New Jersey residents, and researchers can apply for access to specific data relating to their research in a privacy-centric manner. This is a rather novel approach to government-facilitated health data sharing with researchers. Another instance is Massachusetts's All-Payer Claims Database. The database includes data from public and private payers. Differently from the federal Medicare Claims Data database, Massachusetts's all-payer database is provided in a pseudonymized format (rather than an entirely de-identified format) which means that the database retains linkages, providing a more comprehensive dataset that can facilitate research in the public interest. Similarly to New Jersey's iPHD, Massachusetts's All-Payer Claims Database is an innovative approach to government-operated data sharing for research (at least in the United States). The federal government should take notes from both examples as effective ways of protecting patient privacy while supplying researchers with the evidence necessary to advance public health.

—

Here is a timeline outlining the main events discussed above:

Timeline:
February 2009 - The Health Information Technology for Economic and Clinical Health (HITECH) is signed into law, providing funding for the wide scale adoption of EHR

December 2016 - The 21st Century Cures Act is signed into law, setting the agenda for interoperability and data sharing

Early 2018 - The ONC releases their Trusted Exchange Framework and Common Agreement (TECFA), which also establishes FHIR as the US government's preferred API for health information exchange

June 2020 - The ONC Cures Act Final Rule (Information Blocking Rule and further emphasizes interoperability initiatives)

July 2021 - CMS mandates the use of FHIR for data exchange between payers and providers

December 2022 - FHIR adoption becomes a component of the ONC's Health IT Certification Program
—

Among many of the laws and initiatives explained so far, one trend is apparent: the majority of the regulation and rulemaking is voluntary in most circumstances. Aside from the IB rule being enforced across the board and the FHIR mandate among CMS providers and payers, data sharing and interoperability mandates are lacking, even in the public side of the US healthcare system where requirements tend to be more common. Rather, most of the US approach to regulating innovation in the health sector is largely incentive-based. These incentives range from monetary to reputational incentives. While incentive structures can be (and oftentimes are) effective, government-operated incentive programs often fail to keep up with the rapid pace of innovation in the US and global healthcare industry, including private sector initiatives. There are growing private databases such as Epic Cosmos and Truveta that are being used for research purposes using de-identified data. As such, there appears to be an untapped opportunity for the government to partner with the private sector to utilize data sharing and interoperability resources to facilitate streamlined clinical research.

It is crucial to remember that while certain initiatives may not currently be mandatory, they could become mandatory in the future, particularly within the publicly funded healthcare system. Additionally, mandatory initiatives could more effectively expand the United States' health data research efforts. As the history of the US regulatory environment of data sharing and interoperability has shown, shifting from a recommendation/voluntary program to mandatory action happens slowly. For example, FHIR began to gain traction around 2015 and 2016 but was not required by CMS until 2021 (and is still not required for providers who do not accept publicly funded insurance). Progress can sometimes be slow, but requirements often arise with time.

However, innovation does not wait for government intervention. In recent years there has been an explosion in consumer generation of health data that falls outside of HIPAA's scope. This includes data generated through consumer health apps and wearable technologies. While the technology has proven valuable for consumers, the data collected has also proven tremendously valuable for big tech companies and many have taken the opportunity to exploit user data without patient consent. In the absence of comprehensive federal privacy legislation the FTC has taken on the role of regulating health data falling outside of HIPAA. However, the FTC is understaffed and underfunded making it extremely challenging to adequately handle this large responsibility. Moving beyond the scope of the FTC, more is necessary to protect patient privacy while still encouraging data sharing that safely and effectively furthers public health initiatives.

The US has successfully ensured that patients have access to their data. Access by other parties (like researchers) is like a maze where many laws, rules, and agencies create confusion for even industry experts. Looking ahead, the US should now extend access to data to researchers with strong privacy and security safeguards in place. Fortunately, HIPAA provides avenues to disclose health data with public health authorities to advance population health. However, covered entities are not required or incentivized to participate. Nonetheless, many health organizations still opt to share this data anyway with organizations like CMS and the CDC. This broadcasts that healthcare providers would likely be willing to participate in a larger data sharing initiative. The data, however, often lacks standardization, thus inhibiting access. Also, with so much data coming in from many different sources, it has also proven difficult to maintain data quality. Another related issue is determining what level of de-identification is sufficient to enable sharing that is not subject to regulatory restrictions. The Future of Privacy Forum offers an excellent guide for understanding the wide range of practical de-identification options including pseudonymization, de-identification, and full anonymization. Researchers and health entities are still trying to find the sweet spot that protects patients' privacy and autonomy while utilizing data to advance public health.

While this model has created a suitable foundation, there is much work to do to create an effective and privacy-centric health database. As efforts to create a database with clinical value while protecting patient autonomy intensify, they will deservedly raise legitimate concerns from health data and privacy experts. A successful database can only be developed when paired with data sharing, interoperability, and privacy/security mandates. While TEFCA and FHIR are readily available to lawmakers, their effective utilization across the board is crucial, as incentives alone may not suffice. Such an initiative would likely require Congressional support and require an all-around robust regulatory environment that ensures privacy, security, and transparency. To begin envisioning such a project, the US can look to Israel for inspiration.

Israel

Israel has a universal, centralized public health system, managed by the Ministry of Health (MoH) and funded by citizens' health tax and central government budget. Israeli citizens have a unique identification number (given at birth), allowing for effective connectivity between health databases (i.e., cross-referencing and linkage of data about individuals from different databases). While linking health data throughout the healthcare chain typically serves therapeutic purposes and continuity of treatment, these unique features of Israel's health system, and its heterogeneous population, have a significant bearing on the local data environment and make Israeli-based health data research and innovation particularly effective.

Many consider the collection and secondary use of patients' data by health organizations for research and policy-making purposes to be in line with the public interest. This is contingent on the public's interest in protecting its privacy and autonomy with respect to the secondary uses of health data being served.

The Israeli public is medically insured and receives health services from one of four healthcare providers (HMOs), who are licensed and supervised by the MoH. HMOs in Israel have been collecting health data electronically for over 20 years. Their health data silos contain broad data on a large number of patients, ranking at the top globally of quality digital health data repositories. Two of the HMOs, Clalit and Maccabi (which insure approximately 50% and 25% of the Israeli population, respectively), invest substantial resources in developing the collection and use of the data in their possession as well as operate their own research institutes. Consequently, each of the HMOs, which are essentially health data controllers, perceives the health data silos as an exclusive asset, in which considerable resources have been invested in creating. HMOs seek to use the health data in their possession to promote research and innovation within their organization, as well as to improve their efficiency and the quality of the medical treatment provided by them. This is incentivized by the fact that the government awards a budget to each HMO based on the number of insured people who have joined that particular HMO. The result is an incentive for HMOs to promote preventive measures to keep their population as healthy as possible, lowering the cost of care required by each person. This value-based care approach serves as an additional incentive to the shared medical imperative to maintain public health and well-being.

Hospitals and medical centers in Israel are also mostly licensed by the MoH and budgeted by it. They also gather data accumulated in the course of medical treatment and care and during hospitalizations. Some hospitals make extensive use of the data in their possession, promoting innovative research, and also have established innovation hubs that collaborate with Israeli health start-ups that perform R&D together with hospital staff and researchers on the hospital's databases.

Despite the largely positive scene of digitization and innovation in the health sector, there was still the challenge seen by the MoH on a national level, whereas HMOs and hospitals are working mostly in separate silos, and the MoH was setting a goal to promote more collaboration on the national level, in sharing and accessing of health data for research in the public interest, as well as allowing for equal access to researchers of all stakeholders. This policy pursued by the MoH over the past few years is also in line with the OECD Recommendation of the Council on Health Data Governance (OECD/Legal/0433) of 2017.

Keeping this in mind, some background on Israel's regulatory regime concerning the secondary use of big health data for research purposes is described below.

In Israel, the Right to Privacy has been acknowledged as a basic human right in Article 7 of the *Basic Law: Human Dignity and Liberty* of 1992. Personal data is more specifically protected under the *Protection of Privacy Law, 5741 – 1981*, with individual health data considered "sensitive data". Chapter two of the Protection of Privacy Law sets forth the provisions for the protection of privacy in databases, along with the establishment of an enforcement authority, the Israel Privacy Protection Authority at the Ministry of Justice.-

In 2018 a further specific layer of privacy protection was added by the *Privacy Protection (Data Security) Regulations – 2017*. These regulations specify comprehensive data security obligations for databases and apply in a sweeping and binding manner to any activity of processing personal data that is subject to Israeli law, in both the public and private sectors.

The regulations stipulate security level categories for databases, in accordance with their size and the nature of the data contained therein. Databases containing medical data, data regarding a person's mental condition, or genetic data, and which include data about more than 100,000 unique persons, are categorized as "databases subject to a high level of security". The strictest controls and data security measures must be applied to databases belonging to this category, and appropriate obligations are imposed upon database controllers to prevent unauthorized use of data, which is considered a "severe security incident".

Moving beyond privacy-focused legislation, the Israeli legal framework for sharing health data, whether it be through granting access or allowing delivery, is based on the following pieces of legislation:

1. *The Patient Rights Law – 1996*, stipulates that a clinician or medical institution may transmit or release medical or health data to another, inter alia for research purposes and for publication in a scientific journal, providing that patient identifying data shall not be disclosed. The delivery of health data shall be subject to data minimization and purpose limitation requirements, with taking the utmost care in assuring that the patient (i.e., data subject) shall remain unidentifiable.
2. *The Genetic Information Act – 2000,* specifically addresses the delivery of genetic data for research purposes, where it is legally approved research or publication in a scientific journal, on condition that: (1) the genetic data is transmitted without any identifying detail, or (2) the individual data subject has consented in writing to the delivery of genetic data.
3. In addition, since the HMOs and Hospitals in Israel are (for the most part) licensed by the MoH, the law allows the Director General of the MoH to issue Circulars that instruct them on various topics. According to the 2006 *Director-General (MoH) Circular No. 15/06 – Helsinki Subcommittee for Approval of Research That is Not a Medical Experiment in Humans* (IRB Subcommittee Circular), research conducted on data collected from medical, nursing,

> psychological, and other records, that are *strictly a secondary data analysis* without patient involvement or interaction, do not constitute clinical trials in humans.

This creates a somewhat expedited route for the approval of research restricted to data analysis that is deemed to be of *minimal risk*, by an Internal Review Board (IRB) subcommittee. This approach represents the currently applicable legal and policy instrument in Israel, for research using big health data. It should be emphasized that these approvals practically serve as a legal waiver of individual consent for the processing of the data. According to the IRB Subcommittee Circular, other privacy protection and security measures employed are a substitute for consent. For example, if the data is fully anonymized, it does not require consent to be used for secondary uses. This is true in the United States as well. Notably, this does not apply to genetic data research, which is considered much more sensitive and its research requires informed opt-in consent from every individual.

In 2016 the MoH appointed a public committee to examine the implications of sharing big health data and to provide guidance for its secondary uses. This decision was made due to the enormous potential offered by big health data, as well as the benefits of sharing health data held by HMOs with academic and industry research bodies. Underlying reasons for this included wanting to promote the national sharing and access to health data for research in Israel and the "breaking" of organizational silos, as well as promoting the Right to Research in an equal opportunity approach. Thereby allowing access to the budding health startups community in Israel, and giving them an advantage that will push them to be world leaders - access to world-class databases. The committee published its recommendations in January 2018, which sought to strike a balance between the public's interest in utilizing health data and sharing its related research benefits with the rights of individual data subjects to privacy and autonomy. This occurred against the interests of some data collectors and researchers who did not want to make the data accessible.

A government decision 3709 was adopted to make the recommendations of the committee turn operational. One project born out of these recommendations is "Timna" which is a national platform for conducting groundbreaking big health data research. Timna serves research communities in the health system, academia, and Israeli industry. The platform enables the analysis and cross-referencing of medical, demographic, and other data through secure virtual research environments, using advanced methods to complement the data. In this regard, the infrastructure enables access to databases of the Ministry of Health and other government offices for research purposes. Timna's services include hardware infrastructures, software, data security, epidemiological consulting, data science, and data science services.

A request to carry out a study in the MoH will be submitted to the Big Data department in the Computing Division of the MoH through the MoH Big Data Research Portal. Studies carried out must meet the regulatory conditions for data studies, including obtaining the approval of the IRB Subcommittee for each study and obtaining the approval of the MoH Data Transfer Committee. Current big databases made available for research on the Timna platform include data on past hospitalizations in Israel, data on the use of cannabis for medical purposes, data about decedents, and data from infant and toddler care centers. While the Timna project represents a centralized approach driven by the MoH itself to make secondary use of health data accessible to the research community in Israel, another current initiative by the MoH represents a decentralized approach to the data that will be driven by individuals themselves.

To further the mission started by Timna, a draft bill was circulated in early 2023, The Health Data Portability Law Memorandum [2023]. Its goal falls in line with the next generation of innovation in the health sector. This revolution in healthcare is characterized by the ability to collect all relevant health data, analyze it, and derive insights from it in real-time. This serves to improve medical service, increase the therapeutic continuum and the holistic view of the patient's medical affairs, provide innovative and advanced health services, expand the exercise of rights based on medical conditions, and significantly expand the capabilities in the field of research and development. The purpose of the bill is to establish the required regulatory infrastructure so that when a patient wishes to make their data available in order to receive a health service, it will be easily possible at the time and place where the data is required while maintaining the privacy of the patients and the security of the data.

Two key components are required for this:

The first is standardizing and improving the quality of medical data. Bearing in mind that relevant data comes also from outside of the health service providers, from the patient himself, and from various applications and sensors. Although the State of Israel digitized its health records processes relatively early relative to the rest of the world, the data is managed in the various organizations without necessarily employing uniform and modern terminologies, and there are no standard data transfer interfaces. This is a significant barrier to realizing the potential inherent in the data revolution. Even though Israel’s health system is quite centralized, it is divided among many players: HMOs, hospitals, institutes, nursing homes and sheltered housing, welfare institutions, home hospitalization, and more. Alongside these, some players provide services that help with diagnosis, medical treatment, or disease management, such as applications and medical devices. Therefore, lowering the integration barriers through the use of standard and modern data transfer interfaces, and the use of uniform terminology in the system are necessary conditions for effective data portability. The draft bill lays down the regulatory infrastructure for the assimilation of standardization throughout the health system.

The second aspect concerns the regulation required to mandate health organizations to provide the Right to Access the data, and the right to Data Portability, the individual's ability to choose with whom they want to share their existing data. Both rights stem from the Privacy Protection Law in Israel, from the General Data Protection Regulations (GDPR) in the EU, and from laws in countries around the world that have adopted versions of the GDPR. This right is also enshrined in Israel’s Patient's Rights Law. Importantly, these protections extend to all personal data, whereas HIPAA’s right of access only applies to health-related data.

One of the arguments of the MoH in favor of the Bill stems from the structure of the health system in Israel, which is based on "managed competition". Maintaining competition between healthcare organizations is conducive to improving the quality of care and the efficiency of the system. At the same time, this competition can sometimes harm the incentives for sharing the required data between the various players, despite the clear interest of the patients in receiving their data and making additional uses with it, be they 2nd opinion or a 3rd party data-based service. In addition, the MoH believes that even if we assume the "goodwill" of all health organizations in data sharing, allowing broad discretion in the hands of the organizations imposes a heavy responsibility on them and potential liability, which in practice currently prevents data sharing. Every HMO today is required to make an individual decision regarding any data sharing. Healthcare organizations must address privacy and data security concerns, take responsibility for breaches and misuse of data, and adhere to regulations governing data sharing. They then need to invest resources in facilitating data sharing and it's protection in the process. For example, in order to offer the Israeli public an innovative technology-based diabetes management service, the technology company needs to reach an agreement with each individual health organization. Today, the result is that companies will perhaps carry out a pilot with only one of the health organizations, but will not reach full deployment in the health system and in practice will not provide a service to all patients in Israel. To overcome this barrier, the MoH proposes to mandate the HMO to share data based on the patient's consent, (ie. request for access to data and to data portability). The MoH will establish a supervised regulatory arrangement that would grant licenses to entities that request health data. In doing so, the MoH expects to deliver trust between the sources of the data, the recipients of the data, and the general public.

The Bill also builds on work published in Israel in January 2021, by a joint team of the Privacy Protection Authority, the Consumer Protection and Fair Trade Authority, and the Competition Authority, which published a comprehensive document calling for the adoption of the right to data portability as a general right in Israeli law. The right to data portability was defined by the team as a right that "enables a private person to request that it be transferred to his possession, and sometimes directly to a third party, online, so that additional or repeated uses of the data can be made." For this right to be exercised effectively, a person must be allowed to access and port data online in a simple manner, and be able to direct the data controller to transfer the data directly to a third party in a machine-readable format, in a uniform standard, that will make it easier for third parties to make further use of the data. The ability to use uniform standards by all data holders is not a trivial requirement. Standardization requires the ability to reach an agreement regarding the structure of the data transfer and a common language of all those who hold the data and usually requires a significant financial investment in the various data systems, but as the joint team summarizes it: "In the strategic sectors that rely on data for their activities, there is room to consider establishing individual regulation and developing uniform standards to the manner of data transfer in the same market. Determining the aforementioned sectoral policy will take into account the timing and digital maturity of the entities in the individual market, as well as international standards that exist in the field in a way that will allow a cross-border interface." Similarly to the United States, the Bill names the FHIR as the standard for sharing health data. The MoH has been promoting its implementation in Israel HMOs during the past two years together with the FHIR Israel community, and has named the Bill as the preferred choice.

It is interesting to note that this initiative also took inspiration from Israel's Open Finance initiative that was set out about 5 years ago and is performing a similar policy in the financial sector. It is worth mentioning that while preparing this Bill, the MoH simultaneously adopted a lighter incentive-based strategy (incentives like these are standard in the US but uncommon in Israel) to encourage the sharing of health data for research and innovation within the Israeli health sector. The MoH issued a call to HMOs and hospitals, urging them to implement the FHIR protocol in their EHR systems. Additionally, these institutions were encouraged to collaborate with other health entities, enabling research with the data they manage, and thereby making them eligible to apply for dedicated government funding for such innovative big data projects.

Final Thoughts

Israel and the United States have taken different regulatory approaches to facilitating health data sharing. Israel's regulatory framework primarily focuses on requirements, whereas the regulatory framework in the United States is largely rooted in incentives with a few mandates. The United States population is significantly larger than Israel's (36x larger to be exact) and has a primarily privatized healthcare system which makes establishing and enforcing industry-wide mandates a little more complicated. As such, Israel has more legislation that enables easier and broader access to secondary uses of health data for research, including by private sector entities.

Additionally, Israel's comprehensive national privacy legislation could be an advantage in ensuring adequate protections are in place to make patients feel comfortable sharing their health data for research purposes. At the same time, the privacy regulation also offers the tool that Israel's current health data sharing scheme is built upon: the Right to Access and Data Portability. In contrast, the US has a patchwork of health data privacy laws at the federal and state levels, but not a comprehensive privacy protection law. For instance, the right to access exists under HIPAA but is not as wide-reaching as Israel's data privacy law. The lack of a unified framework might be a reason for a lowered level of trust in the US data ecosystem and a deterrent to the wide promotion of health data sharing. Patients may be more willing to share their data for research when strong privacy safeguards are in place, leading to more detailed, prominent, and accessible health data sets and more innovation in the health sector as a whole and for each patient.

Furthermore, one similarity is that both countries struggle with interoperability standards and are both in the process of widely implementing FHIR. With the CMS's FHIR mandate, the United States is currently further along than Israel in its adaptation of the data sharing API.

In conclusion, American and Israeli governments have made substantial progress over the past decade to ease data sharing to improve population health from policy and research perspectives. However, they both have room to grow to ensure that health data is accessible for research in the interest of public health while protecting the privacy and autonomy of individuals.

Throughout this article the terms “data” and ‘information” were used interchangeably based on the choice of the jurisdiction we were referring to. Generally US laws use “information” whereas Israeli laws use the word “data”.