www.jusletter.ch

Florent Thouvenin / Jacques de Werra / Yaniv Benhamou / Abraham Bernstein / Felix Gille / Diego Kuonen / Christian Lovis / Stephanie Volz / Viktor von Wyl

Governance Mechanisms for Access and Use of Data in Public Health Crises: Call for Action

The Covid 19 pandemic demonstrated the importance of access to data to ensure that authorities can make informed decisions in the event of a crisis. However, there are currently three types of barriers preventing access and use of data: (i) technical barriers, especially the lack of uniform data formats and semantics; (ii) legal barriers, especially data protection that limits the use of personal data; and (iii) societal barriers, especially the lack of data literacy and trust. This call for action presents ways to overcome these barriers and proposes new governance mechanisms for the access and use of data in public health crises.

Category of articles: Articles
Field of Law: Data protection

Citation: Florent Thouvenin / Jacques de Werra / Yaniv Benhamou / Abraham Bernstein / Felix Gille / Diego Kuonen / Christian Lovis / Stephanie Volz / Viktor von Wyl, Governance Mechanisms for Access and Use of Data in Public Health Crises: Call for Action, in: Jusletter 17 October 2022

Contents

I. Problem
II. Obstacles
    1. Technical barriers
    2. Legal barriers
    3. Societal barriers
III. Solution
    1. Technical aspects
    2. Legal aspects
    3. Societal aspects

I. Problem

[1] Effective access to and use of relevant data to inform decision making is of utmost importance in a public health crisis. The COVID-19 pandemic demonstrated that access to and use of data on health care, epidemiological indicators, behaviour and mobility, supplies of essential goods for managing the crisis, etc., are not always possible. Furthermore, it was difficult to assess compliance with and the effect of measures taken to curb the pandemic. There are two key problems: First, high quality data is often not available; second, where high quality data exists, it can often not be used in a meaningful way. The COVID-19 pandemic highlighted problems that are also likely to affect responses to other public health crises such as floods, earthquakes, release of chemical pollution or radiation, and power outages. With regard to these examples, we define the term «public health crisis» as an **unusual or unexpected event with potentially severe consequences for the health of a large part of the population**.

[2] The **ideal state of affairs** in fighting a public health crisis is for competent government agencies and other **relevant actors to get reliable answers to relevant questions**. To this end, they must be able to tap into relevant data (personal and non-personal) that is stored with other government agencies or private actors. A promising approach to achieving this goal is to distinguish between data sharing in crisis and data sharing in non-crisis. If these two states are distinguished, there is **no need for prospective data sharing**, i.e. relevant data need not be pooled in a central system, and there is no need to grant access to such data in a state of non-crisis. But there is **need for shareable data**, which requires building an infrastructure and establishing a legal framework that enable data sharing in the event of a crisis. Shareable data may always be useful – but is an imperative in a public health crisis.

[3] In such a crisis, many questions require **real-time and spatially differentiated answers**. For example, where do risks emerge? Who is at risk? How are people at risk behaving? Where are critical assets (e.g. rescue equipment) and infrastructure (e.g. emergency rooms) located and what is their current capacity? Those are just a few examples of questions that would benefit from tapping into existing data streams from individuals, health care providers, private companies, or federal and cantonal government agencies. However, as the COVID-19 pandemic has demonstrated, such data is currently not readily available.

[4] **Three main reasons** inhibit access to and use of relevant data: **(i) technical barriers**, in particular that data cannot be used properly when required to fight a public health crisis, mainly due to difficulties related to reporting and aggregate key indicators; **(ii) legal barriers**, especially through data protection law, which sets narrow limits on the use of personal (health) data, in particular the use of personal data for a purpose other than that for which it was originally collected

(secondary use); and **(iii) societal barriers**, such as a lack of data literacy and a lack of trust in a large part of the population regarding the processing of personal (health) data.

[5] This **call for action** aims to outline the main issues related to effective access to and use of data in a public health crisis, and to present workable solutions to remedy the current shortcomings. It aims to outline a promising approach to fight such a crisis, but it does not discuss specific use cases within the health care sector (e.g. access of government agencies to data collected by physicians). Obviously, the implementation of the approach in Switzerland will have to take into account developments at the international and European level, particularly with regard to standards. While this call for action focuses on public health crises, the approach outlined may also serve as a model for fighting other crises. This call for action does not address the funding needed to implement the solutions proposed by various health care providers such as hospitals, physicians and pharmacies. We are well aware that funding is a key issue, but we believe that it is a political question that must be solved by the competent federal and cantonal authorities. While not addressing all relevant issues, this call for action shows that all present problems could be solved if there were sufficient will to do so.

II. Obstacles

1. Technical barriers

[6] The most important barrier to the effective and meaningful use of data in a public health crisis is the **lack of standardisation**. Data necessary to react to a such crisis is held by various actors such as general practitioners, hospitals, cantonal (health) authorities and federal offices, and especially by the Federal Office of Public Health (FOPH) and the Federal Statistical Office (FSO). These actors use various (medical) data record and management systems («data systems») and data collection processes. The lack of standardisation causes important **lock-in effects**, and the lack of governance and enforcement can further contribute to those effects. Medical data systems are very expensive and sometimes used for many years. Feeding the data is also costly, which is why providers of such systems are rarely replaced. Lock-in effects reduce competition between suppliers of medical data systems, and thus contribute to high prices and lack of interoperability. More specifically, the following technical barriers prevent the use of existing data in a public health crisis:

a. **Lack of machine-readable (structured) digital data**: Much of the data is not available electronically or in a format that is easily machine readable (e.g. physicians' notes). Much is still done by hand. This also applies to notifications that must be made to the federal government and the cantons for certain diseases. In such cases, there is often no electronic reporting option.

b. **Lack of agreement on uniform data format**: The above-mentioned actors store and process data in various formats, thus preventing mutual conversation as the data has no uniform syntax. Although the syntax is often well defined in the medical sector, it is not used consistently.

c. **Lack of agreement on uniform data semantics**: The above-mentioned actors store and process data using individual semantics. Although the semantics are often well defined in

the medical sector, there are several data system providers that apply different semantic standards.

d. **Lack of interoperability**: Interoperability also suffers from the fact that the systems used by the various actors do not have compatible interfaces. Worse, there is no incentive to enable interoperability, and therefore part of the existing software is designed so that data export is not possible.

e. **Lack of data overview**: The use of various data systems also prevents an overview of the kinds of data available and where they can be found. This in turn prevents a rapid response in the event of a public health crisis.

Example
Real-time spatial data on health-seeking behaviour (e.g. purchasing of over-the-counter medications or primary care consultations) may be informative about the local dynamics of a public health crisis. Existing solutions for reporting health data to public authorities (e.g. the Sentinella reporting system for diseases) only cover some of the potentially relevant data. Technical barriers prevent effective access and use of most data that is collected by health care providers (e.g. hospitals, physicians' offices and pharmacies) and by cantonal and federal government agencies.

2. Legal barriers

[7] There are various legal barriers to the effective and meaningful use of data in a public health crisis. Many result from the application of data protection law that regulates all processing of personal data. Anonymisation would allow for an unlimited use of data, but effective anonymisation of health data has become very difficult, if not impossible. Moreover, anonymisation is not always desirable in a public health crisis, as it may prevent health care providers from providing services to individuals in need.

a. **Principle of legality**: The principle of legality requires that government agencies process data only on a legal basis. The use of data by government agencies to fight a public health crisis is often not possible within the current legal framework, as most legal bases for the processing of personal data do not cover such secondary uses. While the federal law on epidemics provides a broad legal basis for the processing of personal data by private and public actors to fight the spread of a communicable disease, there is no such basis for other public health crises.

b. **Purpose limitation**: Several data protection principles complicate access to and use of personal data during a state of crisis. The most important is the principle of purpose limitation stating that personal data may only be used for the intended purpose at the time of acquisition.

c. **Proportionality**: Other problematic principles are the principle of proportionality and, as a consequence, the principle of data minimisation and storage limitation. According to these, data should only be processed to the extent necessary and should be deleted as soon as it is no longer needed.

d. **Discrepancies between federal law and cantonal laws**: The legal provisions that apply to the processing of personal data differ significantly between the federal and cantonal levels, and amongst the various cantons. As a result, personal data can be processed for some purposes by government agencies at the federal level but not at the cantonal level, and vice versa. These differences hinder the exchange of data during a state of crisis.

e. **No crisis mode**: Data protection law applies equally to all situations and does not have any special provisions that would apply in the event of a crisis (e.g. to allow for uses to fight a crisis and to ensure faster action).

Example
In most public health crises, real-time spatial data on health-seeking behaviour cannot be used by cantonal and federal authorities, as they lack a legal basis (principle of legality) and would use data for purposes other than the ones it was collected for (principle of purpose limitation). Furthermore, some potentially useful data (e.g. data on purchasing of over-the-counter medication in pharmacies) may never have been collected or may already have been deleted (principle of data minimisation and storage limitation).

3. Societal barriers

[8] There are also various societal barriers:

a. **Data literacy**: Today, most people perceive the collection and use of personal data solely as a risk and a threat that they cannot understand and control, thereby ignoring that data is a key resource for decision making, research and innovation in the digital society. To overcome this perception, data literacy (i.e. the ability to critically collect, manage, evaluate and use data) must be improved. This also includes the ability to adequately assess and mitigate the risks that may be caused by the processing of personal data.

b. **Public trust**: A major issue is the lack of trust among the public regarding the use of their data by public authorities and private companies. The lack of trust derives from the fact that once the data is disclosed to public or private actors, people no longer know how and to what extent the data flow is controlled, documented and secured. Although this information is provided by public authorities and private companies, the flow of information towards the public seems to be disrupted, leading to public unawareness and lower levels of trust.

c. **Fear of data misuse**: Parts of the public fear that data is used for purposes other than those initially communicated (i.e. that data collected to inform health policy for the public good will be used by private companies for their own benefit). Moreover, the public debate on the collection, storage and use of personal data is dominated by a focus on the risks involved, while the benefits for individuals and society at large are often ignored.

Example
Individuals know little about how private companies and government agencies collect, store and use their personal data. This uncertainty can result in fears concerning data misuse, data security breaches and discrimination, and a lack of overall trust in health system and state activities. This is especially the case for data that is considered to be personal data, such as real-time spatial data on health-seeking behaviour.

III. Solution

[9] The challenges mentioned above can be addressed. Sometimes this can be done through appropriate measures within the respective area, but often combined approaches will be necessary (i.e. measures that affect the technical, legal and societal aspects).

1. Technical aspects

[10] The solution is based on the distinction between **shared data and shareable data**. Data is only shared in the event of a crisis, under certain conditions and in a certain way. Data continues to be stored and analysed in a decentralised manner. Often, shared data no longer has a personal reference. If it still does, privacy-preserving technologies can be applied (e.g. the concept of differential privacy that adds noise to the systems such that the probability that an individual can be identified is kept low).

[11] Shareability implies that data is available electronically, in a predefined format and in an adequate spatial and temporal aggregation, whilst still preserving individual privacy; that it can be aggregated with limited human intervention and in real-time; and that the data or derived results can be shared and pooled on demand through a predefined channel or interface. To overcome the lack of standardisation, **legal provisions requiring and enforcing standardisation** of data formats and semantics in the health sector must be implemented. First steps have been taken in this regard within the federal administration; these efforts must be continued and expanded to private companies operating in the health sector. Standard setting should be a bottom-up process led by the various actors in the health care system, but lawmakers will have to intervene if those actors are unable to define the standards. The standards that are to be implemented make it possible to share and access data in the event of a crisis. In addition, they reduce existing **lock-in effects,** because they ensure lower switching costs and intensify competition. As the nature of a future public health crisis is unknown today, the effort of standardisation should encompass as much data as possible and not be limited to a minimal data set. More specifically, the following are needed:

a. Obligation for all actors in the health care sector to **record all data digitally and in a shareable manner**. Compliance with these standards would serve as a condition for a product or system to be allowed on the Swiss market.

b. Binding standards that ensure data has a minimum **uniform syntax**. Such standards will be implemented through appropriate governance and enforcement mechanisms, in particular through homologation and certification bodies appointed by public authorities (e.g. the specialised body in charge of the management and interoperability of government data).

c. Binding standards that ensure data has a minimum level of **uniform semantics**. Such standards will be implemented through appropriate governance and enforcement mechanisms, as described above. These standards are already being developed in certain sectors (e.g. minimum standards for health-related data from hospitals and laboratories).

d. Systems must be **interoperable** (i.e. have the necessary **interfaces** to communicate with each other). For this, a minimum **interoperability interface** must be defined and implemented by all health care actors. Such requirements will be implemented through appropriate governance and enforcement mechanisms, as described above.

e. The existing obligations to **notify data collections** must be expanded to ensure consistent reporting and an up-to-date compilation of data collections including those of private companies operating in the health sector. In addition, information about interfaces should be provided, to allow for the automated execution of queries during the crisis.

Example
If the solutions for the technical and legal aspects were implemented, real-time spatial data on health-seeking behaviour (e.g. purchase of over-the-counter medications or primary care consultations) would be recorded digitally and in a shareable manner using uniform syntax and semantics. The systems used by federal and cantonal government agencies and private companies active in the health sector would be interoperable, and information about existing data collections and interfaces would be available. This would allow relevant data to be shared in the event of a public health crisis, and enable government agencies and other relevant actors to obtain reliable answers to relevant questions.

2. Legal aspects

[12] While some of the problems require adaptations of data protection law, others may be solved through improved interpretation of existing laws. In general, the focus of data protection law should be less on the regulation (and prevention) of data processing and sharing, and more on appropriate conditions for sharing and processing. The question shall no longer be «if» data may be shared and processed, but «how» it can and should be shared and processed. This includes adequate measures regarding the protection of privacy, particularly regarding data security and the avoidance of specific harm that may arise for the individuals concerned. In addition to the solutions proposed here, certain governance issues must be solved, specifically the allocation of skills and tasks amongst federal and cantonal authorities, and how these authorities cooperate. In addition, it is vital to establish the criteria for defining a state of crisis as well as the authority that applies the criteria and declares the state of crisis. While we recognise that these are key issues, we believe that they cannot be solved in the abstract but must be addressed when implementing the solutions suggested in this call for action. With regard to the legal aspects, the following are needed:

a. A **specific legal basis** for the processing of personal data by government agencies that takes effect in a **crisis mode** must be established. Such legal basis should be provided in federal and cantonal data protection laws to allow government agencies to process all data needed to fight a public health crisis. First steps have been taken in the new Swiss Federal Data Protection Act which will contain a legal basis for the processing of personal data, if pro-

cessing is needed to protect the life or physical integrity of an individual and there is no time to ask for consent. This provision, however, is focused on an individual in urgent need of assistance, and cannot provide a sound legal basis for the processing of large amounts of personal data for the duration of a public health crisis.

b. A specific legal basis for the processing of personal data in a public health crisis would overrule the **principles of purpose limitation and proportionality** with regard to government agencies. A similar result could be achieved for private actors by recognising that the processing of personal data in a crisis can be based on an overriding public interest which would justify a breach of data protection principles. In addition, it must be ensured that no consent of individuals and no approval by ethics committees are needed to process data for the purpose of fighting a public health crisis. In return, processing must be strictly limited to the purpose of fighting the crisis, and the use of data for other purposes must be prohibited.

c. The existing **discrepancies between cantonal and federal law** must be eliminated, and the same conditions must apply to all actors during a state of crisis. A sole competence of federal law during a state of crisis is also conceivable.

d. **A crisis mode** with adequate control measures must be established. In this mode, the government agencies would temporarily have additional competencies accompanied by confidence-building and safety measures. The crisis mode must have a clearly defined wind-down process and/or a sunset date. Additionally, **control mechanisms and compensation options** in the event of harms must be set. A control mechanism could be exercised by the Federal Data Protection and Information Commissioner (FDPIC), which could be supported by a crisis-specific expert panel (with or without decision-making power). The FDPIC should only take decisions after consultation with other relevant government agencies. As always, such decisions are subject to judicial review. The control could be complemented by special **(alternative) dispute mechanisms** which provide for an easily accessible mechanism in case of data disputes, particularly for compensation in the event of actual harm (e.g. in the form of a «lump-sum compensation» for certain foreseeable categories of personality rights violations).

Example
If solutions for technical and legal aspects were implemented, real-time spatial data on health-seeking behaviour could be used by cantonal and federal government agencies on a specific legal basis in the event of a public health crisis, regardless of the purpose for which the data was collected. More relevant data would be available due to the relaxation of the principles of data minimisation and storage limitation. The sharing of data between cantonal and federal authorities would not be compromised by differences between cantonal and federal law. Specific control mechanisms, compensation options and dispute mechanisms would ensure that individuals receive compensation in the event of actual harm caused by the processing of personal data about them.

3. Societal aspects

[13] In general, the public trusts the health system in anticipation of a net benefit for the individual, the public and the system overall. By showing trust, the public legitimises health system activities such as data sharing and data use. Communication of health system actors and the exchange of information with the public about data sharing is critical for building trust. The information that health care actors communicate should describe past comparative positive experiences of data sharing, and present abilities of actors to develop a trustworthy data sharing system in Switzerland and explain future actions on how trustworthy data sharing in the next public health crisis will be achieved. In addition to building trust in the health system, data literacy must be promoted.

a. **Data literacy** must be promoted at all levels of the society. A data literate society would be able to make informed decisions about how data handling (e.g. in the health system) should be organised, to assess the implications of data policy decisions and to evaluate the validity of inferences drawn from data. In the future, data literacy will be as necessary for active citizenship as the ability to read and write.
b. **Public trust** must be promoted by ensuring that individuals are informed about existing accountability and control mechanisms, such as the monitoring of data processing activities of private companies and public authorities by the cantonal and federal data protection commissioners. This could be achieved through an education and information campaign.
c. Such a campaign should inform the public about the benefits of the processing of personal data for individuals and society, the associated risks, and the possibilities and limitations of anonymisation and pseudonymisation. The public should also be informed about existing **measures to prevent data misuse**, how these measures work and what sanctions apply if they are not duly implemented. In addition, the public should be informed about the need to share data in a public health crisis, the benefits for individuals and society, and the specific control mechanisms, compensation options and alternative dispute mechanisms that apply in the event of a crisis.

Example
If solutions for societal aspects were implemented, the use of real-time spatial data on health-seeking behaviour would not only be technically possible and legally allowed, but also accepted by the public. Individuals would better understand how private companies and government agencies collect, share and use data about them to fight a public health crisis. They would also be informed about the specific control mechanisms implemented to prevent data misuse, as well as the compensation options and dispute mechanisms that apply during a public health crisis. Consequently, public trust in the health system would be promoted, even in the event of a crisis.

Annex

Prof. Dr. Florent Thouvenin, Chair for Information and Communications Law, Chair of the Steering Committee of the Center for Information Technology, Society, and Law (ITSL) and Director of the Digital Society Initiative (DSI), University of Zurich.

Prof. Dr. Jacques de Werra, Director of the Digital Law Center (DLC), Faculty of Law, University of Geneva.

Prof. Dr. Yaniv Benhamou, Associate Professor of Digital Law and Member of the Board of Directors of the Digital Law Center (DLC) at the Faculty of Law, University of Geneva.

Prof. Abraham Bernstein, PhD, Full Professor of Informatics, Founding Director of the Digital Society Initiative (DSI), and Member of the Steering Committee of the Center for Information Technology, Society, and Law (ITSL) at the University of Zurich as well as President of the Steering Committee of the Swiss National Foundation's National Research Programme on the Digital Transformation NFP77.

Felix Gille, PhD, DSI Postdoc Fellow, Digital Society Initiative (DSI) and Institute for Implementation Science in Health Care (IfIS), University of Zurich.

Prof. Dr. Diego Kuonen, CEO, Statoo Consulting & Professor of Data Science, Geneva School of Economics and Management, University of Geneva, Co-Initiator «Data Literacy – Switzerland».

Prof. Christian Lovis MD MPH, Chair of the division of medical information sciences, University Hospitals of Geneva, Director of the department of radiology and medical informatics, Faculty of Medicine, University of Geneva, Director of the «Genomics and Digital Health» track of the doctoral school in life sciences, University of Geneva, President of the Iris Fondation, surveillance authority of the shared Electronic Patient Record at Geneva State.

Dr. Stephanie Volz, Attorney-at-law, Scientific Managing Director of the Center for Information Technology, Society, and Law (ITSL), University of Zurich.

Prof. Dr. Viktor von Wyl, Assistant Professor (Tenure Track) of Digital and Mobile Health, Institute for Implementation Science in Health Care, University of Zurich.