The use of data from electronic health records in times of a pandemic—a legal and ethical assessment

Karl Stoeger1,*,‡ and Martina Schmidhuber2,†

1Institute of Public Law and Political Science, University of Graz, Universitaetsstrasse 15/C3, 8010 Graz, Austria
2Chair in Health Care Ethics, Institute of Moral Theology, University of Graz, Heinrichstrasse 78/B2, 8010 Graz
*Corresponding author. E-mail: karl.stoeger@uni-graz.at

ABSTRACT

National electronic health record systems controlled (at least in parts) by the patient are becoming increasingly common. During a pandemic, data stored in such records could be used by health authorities to identify persons with a particular health risk. In this contribution, the authors focus from the perspective of law and medical ethics on the question whether such state access to data could, under certain circumstances, be disadvantageous to a person’s state of health in the long run. This may be the case if the data extracted is not only used for the purpose of informing persons, but serves as a basis for measures taken against the will of the individual concerned. This might be perceived as a “breach of trust” and could result in persons opting out of or not opting into an electronic health record system. Such unintended consequences raise concerns from an ethical and a legal point of view. It follows that, even in times of a pandemic, access to personal data stored in patient-controlled health records should be used as a last resort only. While this contribution deals with the legal framework within the EU,
its considerations are transferable to other national electronic health record systems.

**KEYWORDS:** Covid-19, data protection, medical ethics, pandemic, personal health records, trust

**ELECTRONIC HEALTH RECORD SYSTEMS IN A PANDEMIC**

National electronic health record (EHR) systems containing more or less comprehensive data on a person’s medical history have recently become increasingly popular, as they enable different healthcare providers to treat a patient more accurately by sharing all available health data on this person. At the same time, this comprehensive accessibility of health data raises concerns with respect to data protection. A possible answer to these concerns is the implementation of voluntary participation, be it in the form of an opt-in or an opt-out regime. Another strategy chosen by certain EHR system operators is to limit access to personal data to healthcare providers treating the patients, while state institutions are usually not allowed access to personal data in EHRs. Such EHR systems, which are as a result ‘controlled’ by the patient (either through an opt-in or an opt-out decision concerning all or parts of the content), have been established particularly in parts of Europe. Currently, EHR systems based on an opt-in or opt-out scheme are in operation or about to be established in >10 European states.

---

1. On this advantage, cf. Recital 5 of the Commission Recommendation of July 2, 2008 on cross-border interoperability of electronic health record systems, COM (2008) 3282 final (July 2, 2008).
2. In other words, if a person did not opt into or opted out of a national EHR system, the sharing of electronic health data between different healthcare providers through this system is prohibited.
3. However, anonymized data are regularly available for the purpose of research. Opting-out of health record systems might prove difficult in this context: for the UK, cf. Janos Meszaros & Chih-hsing Ho, Building Trust and Transparency? Challenges of the Opt-out System and the Secondary Use of Health Data in England, 19 MED. LAW INT. 159 (2019). An argument against the necessity of consent for the sharing of data from EHR systems for the purpose of ‘healthcare improvement’ has been presented by I. Glenn Cohen, Is There a Duty to Share Healthcare Data? in Big Data Health Law BIOETHICS (I. Glenn Cohen et al. eds., 2018).
4. On the various systems of (patient accessible) EHRs, cf. Anna Essen et al., Patient Access to Electronic Health Records: Differences Across Ten Countries, 7 HEALTH POLICY TECHNOL 44, 45 (2018).
5. In the context of this contribution, the question that institution hosts the database can be set aside.
6. EHR systems that are, at least to a larger extent, controlled by the patient can be found in several European states. Findings from three sources in English and German (Timelex & Milieu, Overview of the National Laws on Electronic Health Records in the EU Member States and Their Interaction with the Provision of Cross-border eHealth Services: Final Report and Recommendations (2014) https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_report_recommendations_en.pdf (accessed May 28, 2020); Sabrina Bonomi, The Electronic Health Record: A Comparison of Some European Countries, in INF. COMMUN. TECHNOL. ORGAN. SOC. [Francesca Ricciardi & Antoine Harfouche eds., 2016]; Peter Haas, Elektronische Patientenakten (2017), https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/VV_eEPA_Expertise_final.pdf (accessed May 28, 2020)) and additional investigations by the authors show that ‘opt-in’ EHR systems can be found in Belgium, Croatia, France, Norway, Italy, and Switzerland and are...
The comprehensive availability of an individual’s health data in an EHR is not only helpful for patients and healthcare providers, but also in times of a pandemic, it could prove very valuable for health authorities: data on diagnoses or required medication, for example, might be used to identify people at particular risk of being affected by a disease like COVID-19. Identifying these individuals may not only prove useful in the wake of a pandemic, but also after a pandemic’s peak. For example, after a shutdown (which has been imposed in many countries during the COVID-19 pandemic), various protective measures could be taken for these persons, ranging from mandatory home-office to an extended ‘stay at home order’. Several states have already taken such steps recently: in Great Britain, for example, the National Health Service has ‘identified [such persons] centrally by extracting relevant groups from national data sets’; in Austria, the (public) social insurance carriers aim to identify these persons on the basis of state-funded medication. However, the use of these data only allows the identification of risk groups on the basis of rough criteria. Therefore, once the risk factors for a COVID-19 disease (or another pandemic disease of comparable severity) are better known, the use of personal health data from a national EHR system might allow a more targeted approach to identify persons at risk. If the data quality of personal health records is sufficient for this purpose, health records could even be evaluated by Artificial Intelligence, enabling a more rapid and more accurate identification of risk groups.

LEGAL GUIDELINES ON THE USE OF PERSONAL HEALTH DATA

In the following, the use of personal health data from EHRs for the purpose of identifying specific risk groups shall be evaluated from the point of view of law and medical ethics. As a starting point, the authors chose the legal framework within the European Union (EU) Member States. However, the subsequent considerations also apply in principle to any ‘patient-controlled’ EHR system within a state whose national or international human rights instruments permit a limitation of fundamental rights on public health grounds.

Some essential legal requirements for the use of health data by state authorities in the EU can be found in Art. 8 of the European Convention on Human Rights of the Council of Europe (ECHR) and Art. 7 of the Charter of Fundamental Rights of the EU (CFR), which both enshrine the right to private life/privacy, as well as in Art. 8 CFR, which enshrines the more specific right to data protection. Both instruments are binding for all Member States (the ECHR being an international treaty, the CFR being part of primary law, the supreme layer of EU law) and provide a framework for the use of (health) data, which all other pieces of legislation have to respect. In essence, about to be established in Germany (Patient Data Protection Bill by the Federal Government, dated Apr. 1, 2020), whereas ‘opt-out’ EHR systems can be found in Austria, Denmark, Finland, Luxemburg, Spain (partial opt-out only), Sweden (partial opt-out only), and the UK (opt-out beyond direct care).

7 Ruth May & Stephen Powis, Caring for People at Highest risk During COVID-19 Incident: Annex 1 — Identification of Vulnerable Groups: Methods from CMO, https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/2020-03-21-COVID-19-at-risk-Trust-letter_FINAL.pdf (updated May 18, accessed May 28, 2020).
8 Arts. 45 and 46 of the 3rd COVID-19-Act, Federal Gazette, part I, 2020, no. 23.
9 Convention for the Protection of Human Rights and Fundamental Freedoms of the Council of Europe, Nov. 4, 1950, 1953 ETS No. 005.
10 Charter of Fundamental Rights of the European Union, 2012 O.J. (C326).
under Art. 8 ECHR and Arts. 7 and 8 CFR, the use of personal health data on public health grounds by state authorities is only permissible if it is necessary and exercised in a proportionate manner and can be based on a statutory authorization. Such a statutory authorization that is uniformly applicable in all Member States of the EU can be found in Art. 9 para. 2 letter i of the EU General Data Protection Regulation (GDPR), which allows for the processing of personal health data ‘for reasons of public interest in the area of public health.’ This is indeed the relevant legal base for state access to EHRs: despite potential benefits for the individual, using personal health data to identify vulnerable persons in times of a pandemic primarily serves the purposes of protecting the national healthcare system from being overwhelmed by too many patients on the one hand, and of maintaining or restoring the freedom of movement of persons not directly at risk, on the other hand. In other words, the data are accessed primarily in the interest of public health.

According to the above-mentioned Art. 9 para. 2 letter i GDPR, the processing of health data is permissible if ‘processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health’, under the condition that a specific provision has been enacted under EU or Member State law ‘that provides for suitable and specific measures to safeguard the rights and freedoms of the data subject’. Additionally, the third sentence of Recital 46 of the GDPR refers to a situation comparable to the one that is commented on in this contribution: ‘some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread’. Finally, Recital 52 also emphasizes the exceptional legitimacy of the processing of special categories of personal data, including health data, for reasons of ‘the prevention or control of communicable diseases’.

**ETHICAL CONSIDERATIONS**

Consequently, from a legal point of view, access to personal data from an EHR may in principle be permissible in times of a pandemic. However, it is important that the respective statutory provision is proportionate. While lawmakers enjoy a certain margin of appreciation, the advantages of the use of personal data for public health purposes must clearly outweigh the disadvantages for the individual concerned. In balancing relevant arguments against each other, input from medical ethics can be helpful: is it appropriate to value individual privacy interests higher than the public interest in the protection of health? Or should individual autonomy—in particular the right to protection of a person’s health data—be restricted in favor of the common good?

An answer to these questions based on classic moral theories is difficult, because their concepts are unsatisfying in this context: deontology (the Kantian approach)

---

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119).

12 The concept of margin of appreciation was developed by the European Court of Human Rights and is still influential today, for a critical appraisal cf. Janneke Gerards, *Margin of Appreciation and Incrementalism in the Case Law of the European Court of Human Rights*, 18 HUM. RIGHTS LAW REV. 495 (2018).
regards which choices are required, forbidden, or permitted. It determines moral duties and expresses that an action is not subject to any special condition. Only the fulfillment of the duty counts, e.g., saving lives. In consequentialism (utilitarianism) an action will be accepted if it maximizes the good and minimizes the amount of the bad, in other words the greatest happiness for the greatest number of persons. In the actual case of Covid-19, consequentialism would require that the greatest possible number of persons can go back to their ‘normal life’ quickly and that costs in the healthcare system can be minimized at the same time (even if this leads to disadvantages for a minority). Both theories therefore lead to extreme viewpoints: ‘only the duty counts’ versus ‘only the result counts’. As a result, the authors propose to refer to the very influential concept of the four principles of Beauchamp and Childress as it allows balance important moral principles. These principles are autonomy, non-maleficence, beneficence, and justice. All four principles are of equal importance, but must be balanced against each other in situations of conflict, an approach that is somewhat comparable to the legal proportionality test.

‘Informational self-determination’, defined as control over one’s personal (health) data, is of significant value. At the same time, before, during, and after a pandemic, it is also essential that further harm is reduced to a minimum and that all citizens feel treated fairly by the state. While the first phase in countering COVID-19 was characterized (almost worldwide) by drastic measures to reduce physical contact, the focus during the second phase will lie on the gradual restoration of social contacts without causing particular hazards to risk groups, which could consequently lead to overloading the health system. In other words, while initially everyone had to live with severe restrictions for several weeks, the second phase should enable individuals who do not seem particularly vulnerable to gradually return to everyday life. Such an approach is also necessary in order to reduce the economic harm caused by the pandemic and the ‘shutdown’ measures taken in response to it. In this context, it can be regarded as fair (in the sense of Beauchamp and Childress: justice as a fair distribution of costs and benefits) that the autonomy of those directly endangered is affected through the use of personal health data for the purpose of providing special protective measures for them (which, however, do not only benefit them, but the public as well), even if these measures are further reaching than for the rest of the population. What happens here is a trade-off between the interests of the society (economic and health interests) and the vulnerable person’s autonomy. The taking of special protective measures for vulnerable persons allows all other persons to go back to ‘normal life’.

To give an example: a special (extended) ‘stay-at-home order’ for a vulnerable person limits this person’s autonomy, but this order prevents them from being harmed (non-maleficence toward the individual person). Furthermore, this order also prevents that these persons impose various types of costs on society in case of falling ill (non-maleficence toward society). If high-risk persons (elderly and/or with a chronic disease) refuse to stay at home and become sick, they not only risk their own lives, but also tie up resources in the healthcare system. If, however, all persons have to stay at

13 Tom L. Beauchamp & James F. Childress, Principles of Biomedical Ethics (8th ed. 2019). For a critical assessment, however, cf. Katie Page, The Four Principles: Can They be Measured and Do They Predict Ethical Decision Making? 13 BMC Med. ETHICS 10 (2012).
home for an extended period of time to protect the group of vulnerable persons, this will limit the autonomy of all individuals and, furthermore, harm the economy.

However, when taking the principle of non-maleficence into account, there are also convincing arguments against state access to personal data from EHRs during a pandemic. EHRs are to a large extent based on the concept of trust. Users must be certain that their personal health data are only accessible to healthcare providers providing treatment and will not be used by other public or private bodies. The concept of trust is also expressed by the voluntary nature of participation of many EHR systems, namely by opt-in or opt-out regulations.\(^\text{14}\) Trust in an EHR system can be severely damaged by the state if involuntary state access to personal health data may result in measures being taken that the person concerned—despite her or his belonging to a risk group—perceives as disadvantageous (e.g. an obligation to work from home or an extended ‘stay at home order’). From the perspective of the person concerned, cancelling one’s participation in the EHR system might be an appropriate reaction to such a ‘breach of trust’ as this would hinder state authorities from using this person’s data for comparable purposes in the future. State access to personal patient data could also induce other persons to opt out of a national EHR system, or not to join at all. Refraining from participating or opting out of the system will, however, be disadvantageous for these persons from a medical point of view: shared and permanent access to a person’s personal health data by different healthcare providers through a national EHR system is a considerable advantage for patients, especially for chronically ill persons who are vulnerable to certain health risks (including those of a pandemic), as it allows a more accurate treatment tailored to the person’s condition. The disadvantage of not or no longer participating in a national EHR system would persist long after the pandemic and could result in a lower quality of care for the persons concerned. Under the principle of non-maleficence, the state has to take this potential negative consequence of its access to personal health data stored in EHRs into account.

As stressed above, it is not disputed that there is a convincing case for the limitation of the autonomy of vulnerable individuals not only to protect the healthcare system from being overburdened, but also to protect these individuals from a potentially life-threatening disease. However, to limit the impact on their autonomy, such a measure should not be taken on the basis of personal health data that was perceived as ‘safe’ from being accessed by other persons than healthcare professionals. The authors also acknowledge that the possibility to opt in or opt out of an EHR system confirms the state’s respect for a person’s autonomy. However, exactly because of this initial recognition of an individual’s autonomy it seems problematic under the aspect of non-maleficence to counteract the ‘voluntary nature’ of participation in a national EHR system by an involuntary use of personal health data from this system by health authorities in times of a pandemic. While measures restricting autonomy in the public interest are all the more permissible in such a situation, taking them on the basis of personal EHR data should only be the last resort, as otherwise the concept of voluntary participation could be damaged beyond the times of a pandemic.

Thus, state access to personal data in an EHR—which can be justified under the principles of justice and non-maleficence from the point of view of society—may

\(^{14}\) Cf. Essen et al., supra note 4, at 45.
at the same time well has adverse consequences for individual patients under the principle of non-maleficence in the sense that the state should not deter persons from participating in an EHR system. If, however, state access to personal data is only carried out with the purpose of merely informing vulnerable patients, thereby respecting a person’s autonomy and enabling her or him to make their own decisions, state access to health records due to a pandemic is much less problematic and will gain much greater acceptance. Such an approach would also correspond much better with the ethical principles of non-maleficence and autonomy.

LEGAL CONSIDERATIONS
This outcome of an analysis based on principles of medical ethics also concurs with legal considerations concerning the use of health data from EHRs: if the legislator enacts a framework for the operation of EHRs for the benefit of individual patients, and subsequently impairs the attractiveness of these health records by granting authorities access to these records, this legislative strategy must be evaluated through a proportionality test. While it is per se legitimate that the state protects persons identified against their will through coercive measures in the interest of public health, they could at the same time suffer health disadvantages after the pandemic due to opting out of an EHR as a reaction to the coercive measures. This reaction to a perceived ‘breach of trust’ by the state might therefore prove disadvantageous for the person in the long run, as his or her medical history is no longer comprehensively available to all healthcare providers. The same applies for third persons who, after learning of the possibility of state access to stored data, decide not to participate in an EHR system (any longer). While this consequence may be unintended from the legislator’s point of view, it can nevertheless conflict to some extent with—though not violate—positive obligations of the state to protect life or health. It is clear that the state is not obliged to organize an EHR system. However, if such a system has been established, the state must provide a legal framework that allows it to function properly so that patients’ state of health will benefit effectively from the statewide use of this system. This does not hinder the state from providing a possibility to opt-in or opt-out of such a system; rather, by doing so, the state takes into account the fundamental rights of a patient to privacy and data protection. However, when taking measures that make the use of a ‘patient-controlled’ EHR system less attractive (e.g. the use of data from the EHR without consent, even if this use is intended to save lives and consequently in the interest of the patient or the public), the state must always balance the arguments in favor or against such measures.

15 While such positive obligations are recognized in principle, their scope is still unclear and possibly rather limited. In the European Convention of Human Rights cf. David Harris et al., Law of the European Convention on Human Rights 214–16 (4th edition, 2018). For a comparative study cf. Brigit Toebes et al., The Right to Health: A Multi-Country Study of Law, Policy and Practice (2014). In international law cf. John Tobin, The Right to Health in International Law 225–53 (2012).
16 This can be deduced from the case law of the European Court of Justice, which states in essence that while the state is under no obligation to grant a general right of access to healthcare, it must take appropriate steps to protect health and/or life as to the provision of healthcare services in the ‘public health sphere’ (cf. again HARRIS ET AL., supra note 15, at 214). In the authors’ opinion, this also includes the creation of a suitable legal framework for the operation of EHRs if such a system has been established or permitted by a state.
17 In other words, this is about balancing two positive obligations to save persons’ health or lives against each other. While the obligation to save the public from the harmful effects of a pandemic disease is the stronger
at first sight this access seems appropriate due to the protection of public health, its adverse consequence of impairing trust in the confidentiality of data within the EHR system, and therefore deterring patients from using it, must also be taken into account. If this is done, it becomes clear that state access to data stored in ‘patient-controlled’ national electronic health systems to prevent the spread of a pandemic should only be the last option—for example, if this data cannot be extracted from other sources.

CONCLUDING REMARKS

Consequently, when using personal (health) data from national EHR systems to counter the hazards of a pandemic in the public interest, the state is legally obliged—and also strongly advised from an ethical point of view—to reduce potential negative consequences for the concerned patients to a minimum. This means, first of all, that access to personal data in an EHR for the purpose of identifying persons particularly at risk from the COVID-19 (or a comparable) pandemic is only justified if other data that are already available in public registers prove insufficient to attain this objective. Second, state access to such data should only be provided if individual physicians who are bound by professional secrecy cannot easily pass on information to vulnerable persons. Third, if these conditions are met, it must be ensured that such access does not undermine the acceptance of EHRs, resulting in vulnerable persons opting out from the health record system, thereby ultimately harming themselves in the long run. As a consequence, personal data obtained from EHRs in times of a pandemic should, if at all, primarily be used to inform the patient about his or her particular risk, but not as a basis for measures against the will of the concerned patient. If, however, such compulsory measures prove indispensable on public health grounds (e.g. to prevent hospitals from becoming overcrowded with patients from a vulnerable group), it is strongly advisable to base these measures on data over which the person concerned has no ‘data sovereignty’, such as data from mandatory state registers (including information from a public social insurance service regarding, for example, publicly funded medication). This information is not as sensitive and precarious as data from individual EHRs.

one, there is never the less the conflicting obligation not to impair the attractiveness of an ‘patient-controlled’ EHR system as this could in the long run prove disadvantageous for the health of those not participating in the system.

18 In the light of the above-mentioned objective not to undermine the acceptance of EHRs and taking into account the legal requirement to limit the use of data to the minimum necessary (e.g. Art. 5 para. 1b GDPR; ‘purpose limitation’), it must also be ensured that only the vulnerable person himself or herself receives the relevant information and under no circumstances third parties such as employers or private insurance companies.

19 If, for example, it can be established that a certain preexisting condition leads almost inevitably to a serious course of illness that has to be treated in the intensive care unit of a hospital; it will be permissible both from an ethical and legal point of view to temporarily (!) subject the persons affected by this preexisting condition to particularly strict ‘stay at home’ orders. However, this only applies as long as the illness of all these persons would lead to an overcrowding of intensive care units and thus endanger both their own medical treatment and that of other patients.

20 Cf. supra note 8.

21 The sensitivity of data collected in national EHR systems is also implicitly recognized by those states that provide for an opt-in or opt-out of these systems.
Finally, it must never be overlooked that the current pandemic represents a ‘medical state of emergency’ in which the maintenance of public health is particularly threatened. This can serve as a justification for the necessity of (temporary) measures affecting the right to privacy. It is also obvious that such measures are only permissible from a legal and an ethical perspective as long as the disease in question poses a particular threat to public health and the healthcare system. This condition is met in the current situation, as long as COVID-19 is still spreading (even at a slow pace) and cannot be treated effectively and quickly either preventively or after its occurrence. After the pandemic has been managed, personal data in EHRs should be off limits for the state.