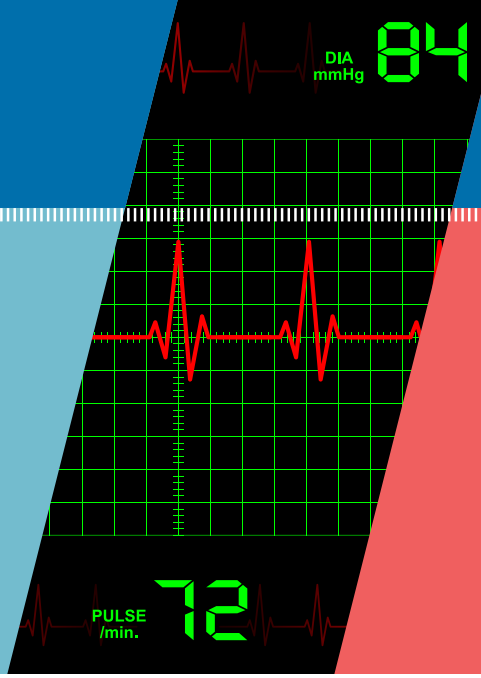


In brief

Health Data

Data on patients' health have been collected for a long time to enable good healthcare for the individual patient and to gain new medical knowledge. In pace with developments in technology and biomedicine, more data, and more types of data, can be collected, stored, combined, linked and analysed in new ways. The potential benefits are huge, but this development also demands weighing up the ethical issues involved.

What is health data?

Health data means personal data* about a person's health status. Health data comes in many forms. What is often meant is data collected and documented in healthcare settings, i.e. the content of medical records and registers of various kinds, doctors' prescriptions, pathology test results, X-ray images, genetic tests, etc. Health data can also be found in other systems such as billing, payments to health service providers, and patient transport booking systems. Health data may also be collected in connection with research, including clinical trials. Individuals themselves are also collecting more and more data related to their own health and well-being through various types of wearables and mobile phone apps. Individuals can also order genetic analyses of their own DNA.

Genetic data

Health data and genetic data are categories that overlap only partially. Some genetic data are also health data, such as the results of certain genetic tests. However, not all genetic data are health data, including data on hereditary characteristics which are not presumed to have any medical relevance, or data relating to parts of a person's DNA that do not encode for any observable traits. A feature of genetic health data is that they can provide information about genes linked with diseases and the risk of future disease.

* Personal data means any information that can be directly or indirectly connected to a living person.

The "In brief" series of publications highlights ethical and societal aspects of a particular topic.

The translation from Swedish has not been reviewed by the Council.

Published January 2023

Health data can provide information about others

A particular feature of health data is that they can provide information about not only the individual the data points relate to, but also about other persons, alive and dead. This is particularly apparent when it comes to genetic information about inherited characteristics.

Where does health data occur?

Health data on all or part of the population is administered by a number of actors. In addition to the various units within the healthcare system, the school health service, and occupational health services, these actors include a number of government agencies, research institutes and providers of allied health services utilised by organisations and individuals. Health data may also be stored within insurance companies and by employers.[1] Data on the health of individuals also occurs in a number of other contexts: in newspapers, on TV and social media, in conversations between friends and acquaintances, etc.

How is health data used?

Health data is a prerequisite for good, safe and coordinated medical care of the individual. It is also fundamental to personalised treatment and the development of precision medicine. Health data can help us to improve prevention tools, for example by making it easier to identify risk groups. This allows screening programmes* to be designed to embrace only groups where these efforts have a clear benefit. Contact tracing for infectious diseases also requires health data. In addition, access to and the collection of health data can help individuals to gain greater control over their health through self-monitoring of vital signs in chronic diseases.

The use of health data is also a prerequisite for following up and developing healthcare, primarily through comparing treatment methods, but also by comparing processes and providers. Health data is also the basis for much of the research that leads to knowledge about the causes of disease as well as effective treatments.

Some important regulatory frameworks

The EU's General Data Protection Regulation (GDPR)[2] regulates the processing of personal data. In principle, the processing of personal data means everything that can be done with the data, such as collecting, registering, storing, linking and merging, or disseminating the data. According to the GDPR, personal health and genetic data constitute sensitive personal data, which means that they may only be processed if certain conditions are met, for example that an explicit consent has been obtained, or that the processing is necessary for reasons of important public interest. In most cases, processing of sensitive personal data requires suitable and specific safety measures. The GDPR is law in all EU countries, but each country can (and sometimes has to) make supplementary laws.

The Patient Data Act[3] specifies how personal data may be processed in healthcare settings. A new Act on shared health and social care documentation has also been adopted, which aims to improve the sharing of data on patients and social care users between the healthcare and social care systems.[4]

The Act concerning the Ethical Review of Research Involving Humans[5] states that if health data or genetic data are going to be used in research, the research must first undergo ethical review and be approved.

The Public Access to Information and Secrecy Act[6] regulates how government agencies may process official documents, which includes the question of when they may release official documents that could contain data about the health of individuals. The Act contains rules on secrecy, and when departures from these rules may be made.

The Biobanks in Medical Care Act[7] regulates how tissue samples may be collected, preserved and used for certain purposes, as well as how the personal data of the tissue donors may be processed.

The Genetic Integrity Act[8] is a single Act covering genetic testing and data within the healthcare system or medical research aimed at providing information about a person's genome. According to the Act, no unauthorised person may gain access to genetic information about another person. However, insurance companies may enquire into and use genetic information in risk assessments for personal insurance for very high amounts.

* Investigations that look for signs of disease in a larger number of symptom-free individuals.

Digitalisation opening up new possibilities

The development of digital technology along with developments in the fields of medicine and medical technology have led to the collection and digital storage of more and more data on the health of individuals. Digitalisation also offers new possibilities for sharing health data between different actors, for example, to improve the treatment of an individual or to enable quality assurance, research and innovation. The development of more powerful computer processors and more efficient algorithms has made it easier to process large health data sets in order to unlock previously unknown correlations that can have an impact on prevention, diagnosis or treatment. All in all, this has led to a growing interest in being able to use digitalised health data in various ways to support health and efficiency in resource utilisation.

An area that requires access to large quantities of digitalised health data is precision medicine, which aims to provide patients with treatment that is tailored to the patient's particular circumstances and needs. Another area where access to digitalised health data is crucial is in the development of automated tools for use in the healthcare system, often based on artificial intelligence (AI). AI algorithms need to be trained with large quantities of data in order to learn how to fulfil their task.*

Processes under way to improve the benefits of health data

A European Health Data Space[10] Work is under way in the EU to facilitate sharing and access to different types of health data – including electronic medical records, genetic data and data from patient registers – with the healthcare system itself (primary use) and for researchers and policymakers (secondary use). Access to health data will be facilitated, while specific safeguards to protect the data will be created.

Genomic Medicine Sweden (GMS).[11] GMS is a national initiative aimed at providing more patients throughout Sweden with broad access to gene sequencing in healthcare to improve diagnostics and individualised care and treatment, and to increase the use of genomics and health data for research, development, and innovation.

Inquiry into more possibilities for the secondary use of data. The Swedish Government assesses that there are currently barriers for researchers, public administration and parts of the healthcare system to sharing health data in a suitable way. The Government has therefore appointed an Inquiry to propose expanded possibilities for using health data for purposes other than those for which they were collected, such as for the care of other patients, and for research, development and innovation. The proposals must take into account the individual's need for protection of their privacy.[12]

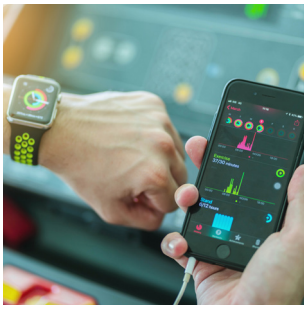
Ethical and social aspects of health data

Health and well-being

Improving health is the most important purpose when health data are processed. For the individual patient, the processing of health data is necessary to be able to make a diagnosis and to decide on, implement and follow up treatment and care interventions. Digitalisation allows healthcare providers to access patient data generated by other healthcare providers, which has the potential to lead to an improvement in the quality of care for individuals. Health data can also help to target prevention initiatives at the right individuals and to make them more efficient. Genetic tests can lead to the detection of phenomena and conditions that can be rectified or alleviated by early detection.

Health apps and wearables that collect health data can assist in the early detection of disease and help patients gain greater control over their chronic illnesses, for example by being able to adjust their drug treatment.

* Read more about AI in the publication *In brief – Artificial intelligence in healthcare* from the Swedish National Council on Medical Ethics (Smer 2020:2).



The processing of an individual's health data can also benefit the health of other individuals, for example by contributing to learning in healthcare organisations. The systematic processing of group-level patient data on treatment methods, outcomes, and complications can assist in weeding out less effective or higher risk treatments. Being able to compare data from many different individuals is essential for tailoring treatments using precision medicine methods. Access to health data is also essential for the development of new and better treatments and more precise decision and assessment tools.

Information overload and health stress

Although access to health data generally makes a positive contribution to health and the quality of care, this does not mean that having as much information as possible is always a good thing for the individual. For example, a genetic test can detect a predisposition for an untreatable disease and the individual is then forced to live with the knowledge for many years that, with some degree of probability, they will develop this disease. In other cases, the data may be difficult to interpret because knowledge is lacking about the strength of the link between a certain genetic variant and a certain disease. The question of what is 'too much' information may come to a head with the precision medicine approach, where large quantities of data are collected to make more accurate diagnoses or tailor treatments for each patient.

Constantly monitoring health status via health apps and wearables could also lead to health stress and to medicalising problems that are fundamentally down to psychosocial factors. Just like other forms of screening, applications that collect and analyse health data with the aim of detecting disease or the risk of disease can result in over-diagnosis and over-treatment and worry people who are healthy unnecessarily.

Empowerment

By providing patients themselves with access to the data generated about them in the healthcare system via their online medical records for example, they can become more empowered in their care, which in turn can improve the quality of their care. Patients can be even more empowered if they are not only able to access health data but can become co-creators of their own health data, for example by reporting inaccurate data in their health records, or uploading data collected through wearables. By being able to share medical records data or data from health apps with other patients, patients can learn more about their diseases and become aware of research projects or alternative treatments.[13]

Privacy and data protection

Data about a person's health is usually considered to be privacy-sensitive data. Some data may be particularly sensitive, such as data relating to mental illness, certain communicable diseases such as HIV, substance abuse and addiction, and sexual and reproductive health.[14] Genetic data, which can provide information about genes linked to diseases and the risk of future disease, may also be particularly sensitive.

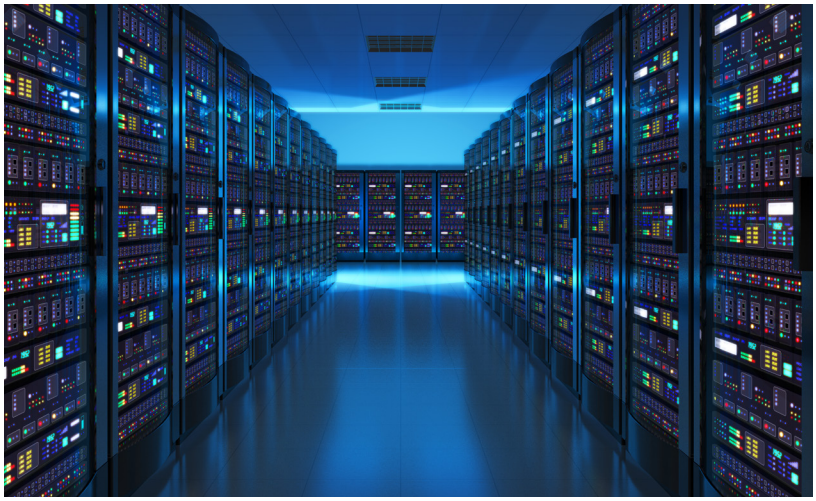
Privacy

Privacy is a concept that is used and defined in different ways. In general terms, privacy concerns the protection of the individual's person, private sphere, and private life. We are assumed to have the right to privacy, but there are different views as to what having this right respected actually means. In the case of private data, for example, some people say that privacy is respected as long as this data is kept from others, while another view is that privacy is protected as long as the individual can control who is given access to the data.[15]

Health data can reveal information about not only the individual to which they refer but also those close to that individual, such as their biological relatives. When it comes to information about communicable diseases, for example, health data may also reveal information about other individuals in the infected person's private sphere.

A person accessing data about another person's health without reasonable grounds may in itself constitute a breach of privacy. The damage that can occur when health data are disclosed ranges from social disdain to stigmatisation, discrimination and expulsion from the person's community. In extreme cases, it can lead to violence related to social norms in honour cultures for example.[16] Other possible consequences of the disclosure of health data are difficulties in getting a job, bank loans or insurance.[17] Digital rights groups have warned that data from period tracking apps that track a women's menstrual cycle could be shared with other actors and used as evidence that a woman has had an abortion in countries where this is a criminal offence.[18] There are also concerns that people with certain diagnoses may be treated less favourably or not receive equal care in other parts of the healthcare system if their diagnosis is disclosed. For many, the consequences might not be particularly serious if their health data fall into the wrong hands, but for some it could be fatal, such as people who live under honour-based oppression or in violent relationships.[20]

Given that data about a person's health are sensitive, all processing of health data requires a trade-off between the potential benefit and the risk of privacy breaches with negative consequences. In order to reduce this risk, the data should not be processed by more people than are necessary



to achieve the intended benefit. The risk of data being disseminated in a way that will harm the individual also needs to be addressed, for example, when patients are given access to their medical records via the Internet.

To prevent health data from falling into the wrong hands, there are strict requirements on the organisational and technical systems that process health data. Weaknesses in data security can lead to the data falling into the wrong hands by mistake, but unauthorised actors can also appropriate the data for themselves from records or registers through active data security breaches. This may include breaches out of curiosity, where the actor in question is just interested in getting information about a particular person, as well as breaches where the intention is to blackmail the individual or organisation affected, or to sell the data for commercial purposes.

"Given that data about a person's health are sensitive, all processing of health data requires a trade-off between the potential benefit and the risk of privacy breaches"

Big Data

The term Big Data refers to the processing of large, complex data sets to detect new patterns and gain new knowledge. The volume and variety of data as well as the velocity with which new data are generated require new methods such as artificial intelligence (AI) for their analysis.

Privacy and Big Data

Many of the benefits that the broader use of health data is expected to lead to in terms of better health and greater efficiency require the capacity to analyse large quantities of data from electronic medical records, health data registers, web platforms, mobile phones, wearables and other sources (Big Data). When large quantities of data about a person are collected and analysed, a person's entire life can be mapped and new sensitive data can be deduced from this mapping, for example, about disease and health. This can include data points collected about the person that taken alone, the person would not see as problematic, such as data registered by wearables. The person might consent to the data being used, but find it difficult to fully comprehend what data they are handing over to another party, and what it might reveal when combined with other collected data.[22]

De-identification

When it is not necessary to know who the health data comes from – as is often the case in research, development and evaluation, for example – de-identification by anonymisation or pseudonymisation can be a means of protecting privacy while enabling the data to be used beneficially. But with sufficient de-identified data from a specific person, it may be possible to re-identify the person (see fact box). As more advanced analysis methods are developed, particularly AI-based methods, and more and more data points are collected on individuals, the potential for re-identification is rising. This is something that could be used by actors interested in identifying individuals, for example, in order to target advertising.

Identifiability, pseudonymisation and anonymisation

Health data are data that relate to an identifiable person (this is what makes them personal data). Some data directly identify individuals, for example, if a name or personal identity number is included. Other data indirectly identify individuals. An example of this kind of data might be: "43-year-old woman born in Örebro, appendectomy 1987, malaria after trip abroad 1999, pregnancy 2006". There may only be one person who fits that description – thus, the woman is indirectly identifiable. It is often difficult to determine whether a certain set of data will enable individuals to be identified. It is unlikely that any individual could be identified based on these data: "52-year-old resident of Gothenburg, complained of cold symptoms in 2019" – simply because there are probably many people who could fit that description. The more data available about a person or the more unique those data points are, the greater the risk that the individual will be identifiable. In some contexts, data points are used that do not in themselves enable identification, but if combined with other data points, they do. When these data sets are kept separate, the former are called pseudonymised personal data. In theory, these data could identify individuals, but measures have been taken to make this difficult. On the other hand, with anonymisation, all data points that enable individuals to be identified must have been irreversibly stripped away. Identification must not be possible with the aid of supplementary data either. Anonymised data is not counted as personal data.

Autonomy

One way of dealing with privacy issues is to require consent for the processing of health data, under the assumption that the individual's privacy is not breached as long as individuals themselves control how their data are used. Requiring consent is also a way of respecting the individual's right to autonomy. Patients' control over their health data may be improved by the option to block access to all or parts of their medical records. Personnel at units other than the unit where the data were collected will then need to obtain explicit consent to access the data in the medical record.

However, we are not always capable of making decisions when we are in urgent need of medical care and health data about us needs to be processed. This raises questions about what the trade-off should be in such cases between on the one hand, care for the patient's health, and on the other hand, respect for their autonomy. Overriding

the individual's control in order to protect their health is usually seen as justifiable, at least in emergency situations.

Using, for example, AI-based tools to predict the future risk of disease through broad analyses of patient data raises questions about what consent ought to be required from the patient and how the patient's best interests from a health perspective should be weighed against the right to refuse medical treatment and to say no to unwanted health information. Monitoring your own health status with health apps and wearables can provide better opportunities for taking control your life, but may also lead to concerns about health taking over your everyday life and in practice limiting your autonomy.

Informed decisions

A truly autonomous decision requires not only that the individual has decision-making capacity, but also information about what the decision involves and its consequences – hence the requirement that consent be informed. Ideally, the information provided when requesting consent for the processing of health data should indicate what data are being collected, with whom the data will be shared and for what purposes the data will be used. As more and more health data are collected and used in more and new ways, this ideal may become more difficult to fulfil.

One problem is that collected health data may be used by many different actors and for many different purposes. The information given to the individual is therefore in danger of becoming overwhelming and difficult to comprehend. This leads to what is called the 'transparency paradox': the endeavour to respect the individual's right of autonomy by providing comprehensive and detailed information in fact risks undermining it.[23] Instead, providing more generalised information that is easier to grasp means that the person giving consent loses some control and must very much rely on the data being processed in ways that they would find acceptable.[24]

Obtaining meaningful consent is further hampered by advances in the development of technologies and methods, which mean that it may be possible to use data in new ways that cannot be predicted when the consent is obtained. In addition, sometimes the purpose of the processing is to identify new unforeseen correlations, which also makes it difficult to fully communicate all the consequences of the consent.

Another challenge is that in some cases it is not possible to say in advance and in detail how the collected data will be used, for example when collecting health data as a resource for future research projects. In research, a 'broad consent' model has been used for some time where the individual, instead of consenting to a specific research project, gives consent to personal data being used for future research for a more general purpose, such as gaining knowledge of causes of disease. 'Dynamic consent' aims to develop broad consent by offering the individual the option of continuously reconsidering their consent choices or consenting to new projects.[25]

Limits of autonomy

Sometimes there is a need to use individuals' health data for purposes that do not primarily benefit the individuals themselves. In these cases, a trade-off may be needed between autonomy and other values such as solidarity and promoting public health.[26] Some purposes are generally considered to be so important from a societal point of view that it is deemed ethically acceptable for the data to be processed without asking the individual for their consent. This applies to the Swedish health data and quality of care registers for example, where patient data are collected in

"A truly autonomous decision requires not only that the individual has decision-making capacity, but also information about what the decision involves and its consequences."

order to monitor health trends in the population and to follow up and develop the quality of care. Under certain conditions, researchers may also obtain data in medical records without the patient's consent but only after ethical review and approval.

The question of how far the requirement for consent should go has become more topical as result of digitalisation and the possibilities it has opened up. The use of individuals' health data is the very foundation of the benefits that digitalisation is intended to generate in terms of health and resource efficiency. For example, precision medicine requires that data from many individuals be compared in order for the right patient to get the right treatment. It raises the question of whether it should be possible to process data from a patient without requiring their consent if the aim is to improve the care of other patients. The care that current patients are offered is based on knowledge derived in part from previous patients. Based on a principle of reciprocity, it has been argued that today's patients have an obligation to help improve the quality of healthcare for future patients, such as by consenting to their health data being processed. This is conditional on the protection of the patient's privacy and other fundamental interests.[27] The problem of obtaining meaningful consent is a factor that has led to a greater focus on solidarity aspects of sharing health data.[28]

An alternative way of looking at the individual's right to autonomy in relation to data about their health that is currently being debated is that instead of the actor who wants to use the data seeking consent for more or less precisely defined areas of application, people should be given more opportunities to donate their data for purposes they want to help.[29]

The issue of an individual's right to decide how their data may be used becomes complicated when the data concerns not only the individual themselves, but may also affect others, such as with genetic data. Should a person be free to share their genetic data if this also results indirectly in the disclosure of sensitive information about relatives? Or if it leads to relatives receiving potentially unwanted information about their future health? On the other hand, should a patient be able to object to healthcare sharing such information with a genetic relative for whose health it may be crucial, or crucial to be able to make a well-informed reproductive decision, even if hiding the identity of the original patient is not possible?

De-identification of data is a strategy to enable the sharing of data when consent cannot be obtained.[30] As described above, it is not always possible to rule out that de-identified data can be made identifiable again, but even where this is possible, it is not self-evident that the individual's autonomy can be casually cast aside. People may have legitimate demands when it comes to influencing how data obtained from them is used – they may want to influence what purposes they wish to support. For example, some may want to contribute to research in certain fields but not in others, or to research carried out by some actors but not others.

Trust

Trust in publicly funded healthcare is based on the care provided being of the highest possible quality. This in turn is dependent on making the most of the possibilities offered by digitalisation. However, if people are going to accept more and more health data about them being collected and used, they need to have confidence that the data will be processed in a way and for purposes that they feel are ethically acceptable. If data security cannot be guaranteed and their health data

"People may have legitimate demands when it comes to influencing how data obtained from them is used."

fall into the wrong hands, if de-identified data are re-identified, or if health data are used in a way that is seen as unethical, trust in the healthcare system and other social institutions could be damaged. This may lead to a backlash where society is forced to impose stricter rules than necessary in order to regain the public's trust, which may lead to difficulties in fully realising the potential benefits of health data.

Retaining trust can be particularly challenging if it becomes increasingly difficult to obtain consent in a way which ensures that the individual understands how their data will be used. If the consent information provided is unclear or difficult to grasp, and it then emerges that the data have been used in a way that breaches a person's privacy, it can lead to feelings of being deceived or exploited, and to a loss of trust.

One way of strengthening trust may be various models that give patients more control over their data by allowing them to track how the data are used for different purposes and giving or withdrawing their consent.

Equality and non-discrimination

One ambition of using more health data is to achieve more appropriate interventions for both individuals and groups. For example, risk assessments based on belonging to a particular group mean that screening programmes and prevention measures can target groups with a high risk of the disease, rather than the whole population, where the risk for many is low. Targeting a screening offer to groups where this intervention would be the most useful could lead to greater health equality and a more efficient resource utilisation. More possibilities for sharing data between different actors can provide a larger patient base on which to perform various types of analysis. This makes these analyses more trustworthy – something that could benefit individuals in smaller patient groups in particular.

But there may also be risks in making assessments of and targeting interventions at individuals because they belong to a particular group. For example, people who belong to groups who are expected not to follow their doctors' orders fully, or who respond less favourably to treatment, or who are at higher risk of suffering from certain diseases, may be at risk of being treated differently than others, not because of traits that they as individuals necessarily have, but because they belong to a group in which such traits frequently occur.[32]

Data bias

Health data collected from various sources are not always representative of the whole population. Some genetic databases have a preponderance of people of European origin, while women and older people are often under-represented in clinical trials.[33] The fact that some groups seek medical care more often than others with similar health problems can also lead to data bias. Genetic and physiological differences between different groups in the population can affect both their risk of becoming ill and how they might respond to treatments.[34] Biased data can make the models developed from this data less accurate for people in under-represented groups.* The result can be that existing health gaps get wider.[35]

Lack of transparency

Automated processes for medical assessments are sometimes based on technologies that are not transparent, where it is unclear what data the results are based on, and how they are evaluated.[36] This can make it more difficult to detect various forms of data bias. The lack of transparency can also make it difficult for people to request a review if they feel that the assessment is incorrect.

"Health data collected from various sources are not always representative of the whole population."

* Read more about data bias in the publication *In brief – Artificial intelligence in healthcare* from the Swedish National Council on Medical Ethics (Smer 2020:2).

Challenges for the future

Digitalisation has brought entirely new opportunities to collect, share and analyse health data to improve the quality of health care and promote good and equitable health. These opportunities need to be harnessed for society to be able to provide care that meets people's needs and expectations. At the same time, the use of health data can bring up a range of ethical issues related to privacy, autonomy, justice and trust among other things. If visions of a data-driven healthcare system are to be realised in an ethically sustainable way, these issues need to be addressed and managed by those responsible at various levels.

PRIVACY AND DATA PROTECTION. Health data are sensitive and can cause serious harm in a person's life if they are disclosed. It is much more difficult today to avoid individuals being identifiable in large datasets. Such datasets can also make it possible to describe individuals from many angles. Given the large quantities of sensitive patient data required to achieve visions of data-driven healthcare, it is vital that questions of data protection and the right of control over data pertaining to one's own health are resolved, and that a solution is found to the question of how data can be shared and made accessible to care providers, researchers and developers in a way that is ethically sustainable.

AUTONOMY. The increased use of health data that can also be linked to data about a person's family members and others close to them affects the scope for respecting autonomy. Applying the principle of informed consent may become increasingly difficult. Should the possibilities of using health data without consent be expanded, and if so, for what purposes? How can this be done in a way that does not risk undermining trust in the healthcare system? Can the patient exercise control over their data in other ways? Should the healthcare system be able to disclose data that can be crucial to the health of close family members but which originally came from another patient?

WHAT DATA SHOULD BE SOUGHT? As more and more health data on individuals are processed, the risk increases of information being disclosed that could in fact be detrimental to the individual. Stands need to be taken regarding which health data should be sought for an individual and how the data should be communicated to the individual or those close to the individual. Patients must be able to make informed choices about what information they want, and their right not to know must be guaranteed.

EQUALITY AND JUSTICE. Increased use of health data can lead to both greater and smaller health gaps. So that everyone can share in the benefits of a digitalised healthcare system on an equal footing, it is important to ensure that the data collected represent the entire population and that the benefits do not just accrue to those groups that supply more health data.

Conclusion

Digital development has resulted in new opportunities for the collection, sharing and processing of data. In the area of healthcare, this can benefit the health of the individual and improve efficiency, but can also entail increased risks associated with fundamental values such as privacy, autonomy and justice. A sustainable approach to the use of health data must be based on a well-considered ethical foundation, in which important values are safeguarded and balanced.

The Swedish National Council on Medical Ethics
(S 1985:A)
smer@gov.se
+46 8-405 10 00
@smer_nyheter
www.smer.se

This publication was decided on at a meeting with the Swedish National Council on Medical Ethics on 28 October 2022. The publication was prepared by the Council's secretariat.

The Council would like to thank Magnus Bergström (the Swedish Authority for Privacy Protection) and Laurent Saunier (Vinnova) for providing views on a draft of this document.

Further reading

Swedish Agency for Health and Care Services Analysis. (2016). *Vad står på spel? Om nyttan med digitala hälsouppgifter och risker ur ett integritetsperspektiv* (What's at stake? On the benefits of digital health data and the privacy risks). Report 2016:3.

Swedish Agency for Health and Care Services Analysis. (2017). *För säkerhets skull. Befolkningens inställning till nytta och risker med digitala hälsouppgifter* (For safety's sake. People's views on the benefits and risks of digital health data). Report 2017:10.

Nuffield Council on Bioethics. (2015). *The collection, linking and use of data in biomedical research and healthcare: ethical issues.*

The Swedish National Council on Medical Ethics (Smer). (2017). *The Quantified Human – Ethical aspects on self-monitoring by wearables and health apps* [English summary]. Smer 2017:1.

The Swedish National Council on Medical Ethics (Smer). (2020). *In brief – Artificial intelligence in healthcare.* Smer 2020:2.

References

1. See the Swedish Agency for Health and Care Services Analysis (2016). *Vad står på spel? Om nyttan med digitala hälsouppgifter och risker ur ett integritetsperspektiv* (What's at stake? On the benefits of digital health data and the privacy risks). Report 2016:3, pp. 27-31.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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).
3 Patientdatalag (2008:355).
4 Swedish Government. (2022, 22 March). *Sammanhållen vård och omsorgsdokumentation* [webpage].
5 Lag (2003:460) om etikprövning av forskning som avser människor.
6 Offentlighets- och sekretesslag (2009:400).
7 Lag (2002:297) om biobanker i hälso- och sjukvården m.m.
8 Lag (2006:351) om genetisk integritet m.m.

9 European Commission. (n.d.). *European Health Data Space* [website].

10 *Genomic Medicine Sweden* [website]. (n.d.).

11 Swedish Government. (2022, 12 May). *Hälsodata som nationell resurs för framtidens hälso- och sjukvård* (Health data as a national resource for the future of healthcare) [website].

12 For example, see *PatientsLikeMe* [website]. (n.d.).

13 See for example the Swedish Agency for Health and Care Services Analysis. (2017). *För säkerhets skull. Befolkningens inställning till nytta och risker med digitala hälsouppgifter (*For safety's sake. People's views on the benefits and risks of digital health data). Report 2017:10*,* pp. 109–110.

14 Anita Allen can be said to represent the first view, while Alan Westin represents the second. See Allen, A. (1987). *Uneasy Access. Privacy for women in a free society.* Rowman & Littlefield, and Westin, A. (1967). *Privacy and freedom.* Atheneum.

15 Sunstein, C. (2001). Privacy and medicine: a comment. *The Journal of Legal Studies*, 30:S2, 709-714.

16 Swedish Agency for Health and Care Services Analysis. (2016). *Vad står på spel? Om nyttan med digitala hälsouppgifter och risker ur ett integritetsperspektiv* (What's at stake? On the benefits of digital health data and the privacy risks). Report 2016:3, p. 69.

17 MacCallum, S. (2022, 5 July). Period tracking apps warning over Roe v Wade case in US. *BBC News*.

18 Mittelstadt, B.D. and Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics,* 22, 303–341; Shilton, K. (2012). Participatory Personal Data: An Emerging Research Challenge for the Information Sciences. *Journal of the American Society for Information Science and Technology*, 63(10), 1905–1915.

19 Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, 140(4), 32-48.

20 Barocas, S. and Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In Lane, J. et al. (ed) *Privacy, Big Data and the Public Good*. Cambridge University Press.

21 Concerning dynamic consent, see Kaye, J., Whitley, E., Lund, D. et al. (2015). Dynamic consent: a patient interface for twenty-first century research networks. *Eur J Hum Genet,* 23, 141–146.

22 Concerning self-determination versus the public health perspective, see Eklof, M. and Normark, D. (2019). Den sjätte medicinen. Den informatiska medicinens kunskapspraktik och etik. (The sixth paradigm in medicine. Practice and ethics in information medicine. In Eklof, M. (ed). *Medicinska moraler och skandaler. Vetenskapens (etiska) gränser.* (Medical morality and scandals. The ethical boundaries of the sciences). Carlssons.

23 Faden, R. R. et al. (2013). An ethics framework for a learning health care system: a departure from traditional research ethics and clinical ethics. *The Hastings Center report, Spec No, S16–S27.*

24 Mittelstadt, B.D. and Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics,* 22, 303–341.

25 Krutzinna, J. and Floridi, L. (2019). Ethical Medical Data Donation: A Pressing Issue. In Krutzinna, J. and Floridi, L. (eds) *The Ethics of Medical Data Donation*. Philosophical Studies Series, vol 137. Springer. Westman, N. (2019, 18 May). 'It's Easier to Donate Your Body to Science than Your Medical Records'. *The Verge*.

26 Barocas, S. and Nissenbaum, H. (2014). Big Data's End Run around Anonymity and Consent. In Lane, J. et al. (ed) *Privacy, Big Data and the Public Good*. Cambridge University Press.

27 Mittelstadt, B.D. and Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics,* 22, 303–341.

28 Rothwell, P.M. (2006). Factors That Can Affect the External Validity of Randomised Controlled Trials. *PLoS Clin Trials*, 1:e9; Devlin, H. (2018, 8 October). Genetics research 'biased towards studying white Europeans'. *The Guardian*.

29 Bentley, A. R., Callier, S. and Rotimi, C. N. (2017). Diversity and inclusion in genomic research: why the uneven progress? *Journal of Community Genetics*, 8(4), 255–266.

30 See Mittelstadt, B. D. and Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics,* 22, 303–341.

31 The Swedish National Council on Medical Ethics (Smer). (2020). *In brief – Artificial intelligence in healthcare*. Smer 2020:2.