CHAIR
DATA PROTECTION
ON THE GROUND

in partnership with BNP PARIBAS FORTIS

Personal data protection in the health sector

Round table report

March 2020

www.dataprotectionontheground.be

ABOUT THE CHAIR ON DATA PROTECTION ON THE GROUND

The VUB Chair "Data Protection On the Ground" (DPOG) promotes the investigation into actual practices of data privacy in organizations and the dissemination of best practices.

The focus of its research is on developments in smart cities, and the health, media, and financial sectors. To this end, the Chair compares practices in public sector organizations with those in the private sector, and organizations experienced in personal data protection with organizations that are making their first steps. In lectures, workshops, roundtables and other events, the Chair brings experts and practitioners together to stimulate the discussion of best practices.

The Chair is coordinated by the research center imec-SMIT (Studies on Media, Innovation & Technology) in collaboration with the research group LSTS (Law, Science Technology & Society), and supported by BNP Paribas Fortis. For more information, please visit the Chair's website at www.dataprotectionontheground.be.

ABOUT THIS REPORT

This report describes the results of a roundtable session that was held in December 2019 and brought 9 representatives from different stakeholder groups together to discuss challenges and solutions for (personal) data protection in the health sector. Participants had been provided beforehand with a policy brief, containing recommendations for policy makers. Under the Chatham House Rule, participants were free to bring in any topics related to personal data protection that they saw fit.

The analysis for this report was conducted by Cora van Leeuwen and Ine van Zeeland, with support from Jonas Albert, Daniela Gallardo Padgett, Myriam Sillevis Smitt and Anouk Verhellen; researchers at imec-SMIT, Vrije Universiteit Brussel.

REPRODUCTION

Reproduction of this report is authorised provided the source is acknowledged.

AUTHORS

Ine van Zeeland
Cora van Leeuwen
Jo Pierson

For questions about this report, please contact Ine van Zeeland, ine.van.zeeland@vub.be.
For questions about the DPOG Chair, please contact dataprotectionontheground@vub.be.

Contents

1. Introduction

The health care sector has faced questions about the sensitivity of data, the meaning of 'informed' consent, and confidentiality for much longer than formal data protection legislation has existed. Nevertheless, the advent of the General Data Protection Regulation (GDPR) in the European Union (EU) has raised awareness of such topics to the surface level of discussions within health care facilities and between health care professionals and patients.

On 11 December 2019, the VUB research chair on Data Protection on the Ground organized a round table discussion between Data Protection Officers from the realm of hospitals and health insurance, specialized legal academics and legal professionals, and representatives of patient organizations in Belgium. The overarching theme was 'personal data protection in the health sector' and in three rounds participants discussed the main challenges and solutions.

"The concept of sensitive data will have an inflation effect
were almost anything which is big data will be sensitive data."

Participant quotes

This report will go into the main themes that emerged during the round table:

- explaining what happens with health data (§2)
- legal concerns and misconceptions (§3)
- corporate possession of health data (§4)
- sharing data internally and externally (§5)
- using health data for research (§6)

The discussion also yielded insights that promise avenues for solutions to data protection challenges in the health sector, which were mostly centered around training and education for various different groups. These suggestions will be presented at the end of this report.

2. Explaining what happens with health data

For patients, it is often not easy to understand what happens with 'their'[1] health data, for various reasons. For example, when health data are used in big data research, researchers sometimes also don't know yet which correlations may result from a machine learning process, or how the process itself works exactly. As a consequence, they won't be able to fully explain how health data are used or what the consequences may be (see §6). Nevertheless, even in these complex circumstances an explanation is owed to the patient. One participant underlined that if something unexpected comes up in genetic research, such an incidental finding should be communicated to the patient, even if (as another participant pointed out) it isn't easy to find a good moment for this communication.

Several participants argued that standardizing explanations should be possible, for example in the shape of a one- or two-page document using language that is easy to understand. This standardized explanation document (template) could be hospital-specific, but criteria for standardization could also be drawn up at a national or European level, in the sense that the type of information to be included in the explanation should meet common standards. For instance, information provided to participants in clinical trials could easily be standardized as the information will be very similar in most situations.

[1] There was not much discussion during the round table about which data can be considered to be the data of an individual patient, but this can be an interesting disambiguation discussion in itself.

Alternatively, the patient can be given a summary explanation and a link for follow-up information. Since health data may be used and re-used, an online source that is constantly updated with the uses and results could be helpful in explanations, as well as to manage 'dynamic consent' so the patient can restrict certain types of re-use. It is re-use in particular that patients may not be aware of, so it will be important to make this clear to them. In fact, some round table participants implied that the focus should be moved from explanations to transparency, as this will also help address trust issues (see §5).

"I would not say that informing people is a lost cause. There are other things you can do."

The other side of the explanation coin is the understanding of the patient. For one thing, people who are ill may not be capable of understanding what happens with their data, or even interested in hearing about it. For another thing, the question is whether explanations are meaningful to patients. Information may be meaningful to some patients but not to others. For instance, patients with dementia are a challenge for the provision of meaningful information. Some participants in the discussion argued that while patients may not understand everything, they still have a right to know what happens with their data and that paternalism would be misplaced. Patients can look up what they don't know or ask other care providers for help. One participant mentioned that patients with a rare disease may even be more knowledgeable about the specificities of that disease than their GPs.

Explanations are a necessary component of consent from the patient if that consent is to be valid under the GDPR.[2] At the start of the discussion, a participant made clear that there are many misconceptions about 'informed consent' in health care settings; first and foremost the misconception that consent from the patient would always be needed to process his or her data. There are many health care situations in which the patient's consent will not be needed at all. The most notable one is an emergency situation in which the patient's life is at stake. As two participants remarked, the legal ground of 'vital interests of the data subject'[3] was specifically included in the GDPR with these medically urgent situations in mind.

"When you are really ill and fight for your life you don't care about your data."

According to some participants, misconceptions about consent are perpetuated by ethics boards, who sometimes push for consent even when it is not appropriate. Even for research, consent from the patient is not always needed as a legal basis for processing personal data. Participants also pointed out that there are so many different types of consent – contractual consent, clinical trial consent, consent to a specific treatment, consent to process personal data – that confusion may arise with regard to what exactly it is that a patient needs to agree to.

In Belgian hospitals, most patient data processing activities are carried out on the basis of other grounds than consent, for example based on a contractual agreement or the patients' vital interests. When they register in a hospital, patients are asked for consent to sharing of their personal data with other healthcare providers and hospitals through the eHealth data-sharing portal. In general, the problem with obtaining valid consent from patients is that they just want to get better and cannot be bothered to consider what happens with their data. In that sense, the criteria for valid consent can

[2] The conditions for valid consent under the GDPR can be found in Article 7 and Recital 32 GDPR and include the condition that consent be *informed*, in other words, the 'data subject' must understand what is agreed to.
[3] Article 6(1)(d) GDPR.

often not be met in health care – too much is at stake for patients. One should also consider that patients who need to trust a doctor with their lives will extend that trust to governance of their data.

There will be different purposes for health data and even if separate consent were to be asked for all of those, patients would not have the peace of mind to carefully consider which they would agree to and which not. In addition, verifying that someone has understood what they were agreeing to, as required in a strict interpretation of GDPR consent, will be very impractical.

"Will people need to do an exam before they can give their consent?"

In the context of informed consent, the issue of health care providers not being able to specify beforehand what exactly will happen with health data and who will have access to it, crops up again. In the course of treatment, as someone's developing condition is studied and monitored, various specialists will have to take a look at medical data ('a multidisciplinary health trajectory', in the words of one participant). Pharmacists (who need to prevent contraindications), financial administrators (arranging reimbursements) and other hospital staff will also have to access the patient's data.

A related topic that came up in the discussion was that people will often share a lot of data that could be considered health data with providers of smartphone apps and (fitness tracker) wearables. The risks for these kinds of data sharing look remote and people rarely ask where the data go. Awareness about the protection of health data in these circumstances should be raised among the general public.

3. Legal concerns and misconceptions

As was mentioned in §2, there are many misconceptions about the GDPR.[4] As one participant remarked, some people think that no personal information can be shared at all anymore, out of fear for fines under the GDPR. Different platforms for storing patient data developed at the Flemish and federal level in Belgium turn out to have different approaches to and interpretations of GDPR requirements, and there seems to be no answer to the question of who is right. Answers about 'correct' interpretations are expected from the Data Protection Authority (DPA), since the DPA will ultimately hand out fines, though one participant had reservations about asking recommendations from the authority that also hands out the fines. Another participant pointed out that litigation by patients is also a possibility, but they will have to demonstrate suffering harm from a data breach.

Example given in discussion

A doctor wants to share information about a pregnant patient's condition with her mother who lives abroad but hesitates between sharing that information over the phone or over email and chooses not to share any information at all out of prudence. As participants explained, sharing such information over the phone would be more protective than sending email, since digital information in email can be copied and forwarded more easily, and email invites over-sharing because of the ease of attaching full documents.

Participants drew attention to the fact that authorities in different EU countries enforce the GDPR differently. The lack of pan-European agreement on GDPR enforcement was not considered to be conducive to finding solutions to data protection issues. GDPR enforcement was considered necessary to achieve any change. Besides, breaking the law should not be without consequences.

[4] Previous round table reports about data protection in the media sector, smart city projects, and the financial sector will underscore this issue. These reports can be found under 'Publications' at www.dataprotectionontheground.be.

The fact that other regulations affect the health care sphere and lead to different interactions with data protection in different countries, was readily acknowledged in the discussion. Such other regulations may apply to safety for medical devices, discrimination, contract requirements, and medical confidentiality. If it is difficult to harmonize regulations within a country, then it will be even more difficult to attain harmonization at a European level. Beyond laws, differences in health insurance systems will also affect practice. As a consequence, guidance should still be provided at a national level or, as some participants suggested, at a sectoral level. As an example, the Dutch federation of hospitals has created its own service to quickly answer GDPR questions and raise awareness.

"You also have anti-discrimination laws. In Belgium, you cannot use medical information to discriminate."

4. Corporate possession of health data

Companies like Google claim that they are capable of predicting health outcomes based on search data combined with troves of personal data from other sources. Some of these data would not be considered as 'health data' at face value, such as location data gathered by apps. Large 'big data' corporations hoard valuable data and restrict access to serve their own interests, which is unfortunate for (academic) researchers. Individual hospitals or research institutes cannot address this situation on their own. There should be legal provisions to regulate which health-related data can be locked up and which should be shared (see §6).

Users of mobile apps or mobile medical devices are often unaware of this type of data collection. When they do find out, e.g. by reading the fine print in privacy policies, they may lose trust in health-related research.

Hospitals may also enter into agreements with commercial providers that entail sharing health data with commercial third parties. In some cases, such contracts are not completely clear on which party is the controller and which party is the processor of personal data and this may lead to various problems, e.g. lock-in situations for hospitals that can no longer access patient data unless using the provider's services.

The health insurance sector is a special case. As health insurance providers are legally required in Belgium to offer insurance to everyone, excluding certain groups is out of the question. Therefore, health insurance providers are looking for profit elsewhere by analyzing the data they hold. These analyses could also have public benefits, e.g. in prevention. Using the insights gleaned from health insurance data in any discriminatory manner is, of course, prohibited.

Example given in discussion

Company A did a proof-of-concept study in a Belgian hospital on glycemic analysis of patient data collected with mobile devices. The data were transferred to A in their processor role, but A subsequently declared itself controller when it came to the use of the data. Doctors and patients at the hospital can no longer import or use the data directly, only via A. Health care professionals have to log in to get access to glycemic values of patients, which is experienced as cumbersome.

Meanwhile, patients have grown accustomed to using A's devices and the benefits of their use would be lost if they were to be replaced. Moreover, the devices are implanted and would require surgery to remove.

Participants in the round table felt that using health insurance data for public benefits would indeed be laudable, but they were skeptical about other uses. While direct discrimination is prohibited, it would, for example, still be possible to disincentivize some groups by offering additional refunds that only appeal to other groups, as learned from big data analysis. If this occurs structurally in society, this will create inequality in insurance benefits.

"Being more up to date on health practices or activities we want to stimulate in the public by the incentives that are given by the government, is going very slow. And that is where [health insurance providers] say they can do it faster, but they also have these other goals."

Some participants argued that health research is simply not a task for health insurance providers. Patient data is provided to the health insurance providers to allow for correct reimbursement; these data should never be used for commercial or any other purposes, while other participants suggested that health insurance data should be open data or that umbrella organizations like RIZIV should be responsible for population-level research with health insurance data.

5. Sharing data internally and externally

Some of the discussions above already hinted at issues surrounding the sharing of health data, but this was also an important topic in itself during the round table. Health data can potentially be shared within an organization or between different organisations. However, exchanging health data between specialists in different hospitals is difficult even when the data are de-identified and even when the sole intention is to improve a treatment. This is not only due to the GDPR, but also due to medical confidentiality regulations. Data sharing platforms are incompatible, hampering organizations' willingness to share data.

Hospitals generally log access to patients' medical files. Patients have the right to request those logs, but in practice, few do. They may be surprised to see how many different health care professionals access their files, but as has been explained in §2, all kinds of professionals need to access those files for purposes of integrated care, financial reimbursement or verification of contraindications of medicine. The Belgian Health Care Facilities Quality Act of 2019 describes medical files and its interpretation of the 'therapeutic relationship' needed to access files is: everything that is needed for health care. The logs do provide a means to limit unnecessary access, as health care professionals are aware that their access is logged. If unauthorized access is suspected, it will be discussed.

Example given in discussion

In a Dutch hospital, an inordinate number of staff had accessed the medical file of a celebrity who underwent treatment there. The hospital was penalized by the Dutch DPA, but there was some discussion of whether individual staff should have been penalized instead. Round table participants felt that the hospital was indeed the main controlling entity responsible for managing data access.

Governance and management of health data should receive more attention. Hospitals should have solid policies about data governance: if professionals get access to medical records, they need to be able to justify that. In the discussion about access, for instance, one might ask if everyone who has access to a patient's file needs to have access to the full file or to only parts of it. Participants felt that within a hospital it should be possible to ascertain what happens with personal data and give a complete overview to a patient, but managing access becomes a lot more difficult when the data are shared outside the organization, for instance with a research institute. Good contracts or data sharing clauses are important, but without controls agreements are hard to verify.

"If things are well logged, access should be broad. There is a chance to reduce misdiagnosis and a risk of overlooking problems if access isn't broad enough."

Trust is a key aspect of this discussion. Hospital patients are usually willing to consent to sharing their data between their doctor and other health care professionals within the same hospital. Some patients don't trust sharing of data with third parties, especially not if they feel that this happens 'behind their backs'. If they find out about 'their' data being shared with others without their knowledge, they may become reluctant to share information about themselves, which in a health care setting can be detrimental to their health.

Balancing the pros and cons of sharing health data is therefore an exercise that needs to be elaborated more. The GDPR prescribes Data Protection Impact Assessments (DPIAs) for new activities involving the processing of health data but is not specific enough on how these should be carried out and how to assess risks. There is some debate on whether traditional, quantitative risk assessment approaches, involving an assessment of likelihood and severity of a risk, are applicable when it comes to the protection of fundamental rights like the right to a private life, which cannot be quantified.[5] An example mentioned by one participant was that if a researcher collects data about a certain group, this might lead to stigmatizing thoughts about this group e.g. that they are engaging in risky sexual behavior. The likelihood or severity of that risk would be difficult to quantify or reduce to financial costs. Round table participants seemed to be in favor of a more cautious approach to DPIAs; current implementations should be tried and tested for a longer period of time before new formal requirements would be added.

"By making it more quantitative you give the impression that it is more correct, where it is not. It is still an estimation, a feeling."

Organizations' data protection officers advise on DPIAs and monitor data protection practices of the organization. If a DPIA is not carried out correctly, the data protection officer can theoretically contact the DPA (with approval from his or her employer). As several participants pointed out, this may lead to a conflict of interests. Data protection officers are supposed to be 'independent', but will the data protection officer of Google tell Google not to combine lifestyle data with search data to deduce health issues? A data protection officer will have affinity for the organization he or she works for at the very least; true independence is unlikely. The advice of data protection officers may also be overruled in board rooms, where different interests wrestle for precedence. In the absence of enforcement, data protection concerns are not likely to win there.

6. Using health data for research

Sharing data for health research has been discussed in several places above, but there are still a few remaining comments on the topic.

People who have a rare disease often advocate for lower barriers to health data sharing, as more sharing of health data would promote a faster development of treatments. Data from healthy people also help towards such efforts, as these can create baselines. Healthy people, on the other hand, are

[5] E.g. in: Dijk, van, N., Gellert, R., & Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*, 32(2), 286–306.

often disinclined to share health data, as they see little benefit to themselves, but they do see increased risks.

While protection of health data is important, so is opening up health data sets to advance medical research. Several participants argued for more access to health data. There should be legal provisions on a European level to standardize and guarantee access to health data for research purposes, to make sure that more data sets are open – not only data collected by researchers, but also data collected by corporations.

On the other hand, aside from the issues with data sharing platforms described in §5, there are other challenges to sharing health data for research. Aggregated data sets need to be created, maintained and standardized, but there is no clear allocation of responsibilities to achieve that. De-identifying data is a complex process and anonymity is hard to guarantee. There are also issues with the quality of open data.

7. Suggested solutions

As indicated in §3, transparency was mentioned repeatedly as a solution to explainability issues as well as problems around consent. As one participant argued, consent boils down to the reasonable expectations of the patient: Context matters to what is reasonable to know for people with different roles in the hospital. What kinds of access are acceptable depends a lot on what a patient would expect should he or she understand all the details and nuances. If the relationship between the doctor or hospital and the patient is transparent, the requisite trust can be created that will pre-empt the need for consent. It is not helpful or reasonable to expect patients to read a 50-page privacy policy – they should be able to trust health care professionals with their data, as they already do with their lives.

This will require sufficient knowledge of data protection among health care professionals. The need for training of health care professionals in data protection, or at least digital literacy was highlighted several times in the discussion. Training would have to be role-specific rather than generalized for the whole organization to be of most practical use for health care professionals and to directly applicable. Data protection or digital literacy training should maybe be part of health care education.

For practical questions and advice, such solutions as a ‘GDPR hotline’ and a national website answering frequently asked questions were suggested, since both would also be useful for independent general practitioners and care homes. Sector organizations could be the driving force behind such initiatives.

Not only health care professionals should be trained, ethics boards also need to be educated in disambiguating different types of consent. Even legal departments were mentioned as an audience for training in personal data protection, as they are often focused on checking other aspects of contracts while overlooking data sharing clauses. One participant suggested that executives of organizations should be trained in data protection too.

As in previous round tables, the need for digital literacy education in primary and secondary schools was mentioned several times. People need to know more about the risks of digital data collection and about the rights they have to the data that are processed about them. Another recurring appeal is the need for enforcement, to clarify requirements and raise awareness to change corporate culture.

8. Conclusion

The health care setting poses a specific challenge to obtaining consent from so-called 'data subjects', the patients. The discussion also made very clear that explanations, while sometimes challenging to provide, are of the utmost importance to create and maintain trust. On the other hand, awareness of personal data protection should be raised throughout society and education, and enforcement plays a central role in achieving that ideal situation.

Subsequent research
Based on the challenges and solutions highlighted in the roundtable discussion, subsequent research will focus on the issue of consent and to what extent understandable explanations and transparency can replace the need for consent. These research efforts will be conducted within the framework of the research chair Data Protection On The Ground.