Interdependent Privacy & Medical Information

Valérie Junod*
Professor at the Faculty of Business and Economics (HEC) of the University of Lausanne
Professor at the Law School of the University of Geneva
Junod, Muhlstein, Lévy & Puder, Geneva

Sami Salihu
BLaw, University of Lausanne
Research assistant at the Department of Business and Tax Law (D-DAF) of the University of Lausanne
Legal intern, Bratschi Ltd, Lausanne

Keywords: Medical information, Interdependent privacy, Controller, Insurance, Research

Abstract: Data protection laws are typically conceived around the relationship between one controller and a single data subject. In other words, a data subject is given rights against a controller (or possibly a processor), whereas the controller has corresponding obligations. However, there are a number of situations where the data at issue does not only concern a single data subject, but a group of interrelated individuals. This article focuses on three medical settings – health care, insurance coverage and research – where an individual (the first data subject) holds and communicates to the controller data which, directly or indirectly, relates to a third party, often a family member. The best-known example of such data is of course genetic information which is by definition shared among most family members. How does Swiss law, chiefly the (current) Federal Act on Data Protection, handle such triangular patterns and what could be improved are analyzed here.

Table of Contents

I. Introduction

At the doctor's office, patients are commonly asked whether their family members, partners or other contact persons have suffered from certain disorders, such as cancer, cardiovascular[1] and/or transmissible diseases.[2] This information can be highly relevant to determining the care or the medical supervision that patients need.[3] It is then kept in the patients' medical files. From the physician's perspectives, it is good medical practice to ask, to record and to use such information.[4] Failing to do so may make the health professional[5] liable,[6] should this lead to harm and damages.

* V. Junod thanks Prof. K. Huguenin (HEC, Unil) for the thoughtful comments kindly provided on the draft.

[1] Many diseases (and predispositions to disease) have a genetic foundation and thus can be "inherited" by family members. This is the case, for example, with cancer. See *e.g.*, Chappuis P.O., *Plaidoyer pour l'anamnèse familiale… à l'ère de l'oncologie moléculaire,* in: *Rev Med Suisse,* Vol. 1. 30408, 2005.

[2] *Contact tracing* in the COVID-19 context is briefly addressed in the conclusion (*cf.* Section V). Other transmissible diseases, for which a contact history can be highly relevant, are of course sexually transmitted diseases.

[3] Bochud M./Waeber G./Vollenweider P., *Anamnèse familiale: utile ou futile?,* in: *Rev Med Suisse,* Vol. 5, 2009, pp. 263–267; Académie Suisse des Sciences Médicales (ASSM), *Potentiel et limites de la «médecine individualisée» (personalized medicine),* Feuille de route, 2012, p. 7.

[4] Article 40.a of the Federal Act of 23 June 2016 on Medical Profession (CC 811.11) – indirectly, see also Articles 4.2 and 6; Article 3 of the Code of Ethics of the FMH Swiss Medical Association.

[5] Our article focuses mostly on medical doctors (physicians), but other health professionals are typically subject to the same privacy rules. How they interact with patients may vary, however. For example, a pharmacist is probably less likely to ask clients questions about their family members or contact persons.

[6] According to Article 398.2 of the Code of Obligations of 30 March 1911 (CC 220), the doctor, as an agent, "is liable to the principal [the patient] for the diligent and faithful performance of the business entrusted to him". In order to properly fulfill her legal (and contractual) obligations, the doctor is supposed to gather as much relevant information as possible about her patient.

Similarly, a (private) *insurance* company may ask their prospective clients whether family members have been diagnosed with certain medical conditions.[7] From this information, the insurance can try to infer the client's risk of early death, disability or added medical expenses. It can adapt the insurance premiums or refuse coverage accordingly. This information is typically kept in the insurance file of the client, sometimes even if the insurance proposal is ultimately not signed.

Finally, in *research* settings, it is common to gather information about family members of research participants, because this can help refine the analysis of the collected data and therefore improve the reliability and relevance of the research results. This information is also retained by the researchers.

These three fact patterns raise at least four key issues, analyzed in the following sections. First, is the patient/client/research participant (hereafter: data subject 1 or DS1) *allowed to provide information about family members* (hereafter: data subject 2 or DS2)? We here mean data that concerns either DS2 (alone) or both DS1 and DS2.[8] Second, is the doctor, insurer or researcher (hereafter: controller 1 or C1) *allowed to ask and then store the answers* provided? Third, *can C1 herself use this information for purposes unrelated* to the initial relationship with DS1? For example, if the doctor is also caring for the sister of the patient who provided the information, can she use it to improve the care of the sister? Fourth, *can the recipient of the personal data (C1) share it with other parties* (hereafter: controller 2 or C2), who might have a use for it?

Although these four questions are quite ordinary, their answers are far from straightforward. They involve the delicate issue of interdependent privacy.[9] By this we mean that DS1 is not releasing personal data (only) about herself, but also about DS2[10]. Most often, DS2 is not even informed of this communication.[11] Since she does not even know that her privacy may be threatened, she has little ways to defend her rights.

The present article focuses on Swiss law, excluding issues related notably to the GDPR. Genetic data is viewed as one kind of medical data at issue; our focus is broader, however.

II. Communication by One Data Subject of Information Concerning Another Data Subject

In the course of ordinary life, we routinely disclose personal information about third parties. For example, one office worker may say to another, "Did you notice that John came late this morning?" or "Do you know that Jane is about to go on maternity leave?" or "Let me introduce Jack, he used to work for this other company based in Dublin". This is part of ordinary conversation and gossip. We do it at work and in social settings, without giving it any thought. Sometimes, the person we talk about is present, sometimes not.

Gossip may be viewed as inelegant, but it is rarely thought of as illegal.[12] Yet, applying the Swiss Federal Act on Data Protection (FADP)[13], a person communicating personal data about another person to a third party

[7] Groupe Mutuel, *Protection des données: Position du Groupe Mutuel,* Martigny 2014; Generali Suisse, *Informations sur la protection des données,* Adliswil 2019; On the Swiss Insurance Association's website, there is a standardized form *("Aerztlicheruntersuchungsbericht"* or *"Rapport de l'examen médical")* for the private insurance companies: on this form, *Question 8* asks for information about family members' health, more specifically whether "your parents, siblings or grandparents had any diseases of the nervous system, cardiac diseases, strokes, diabetes, cancer or hereditary diseases before the age of 55? Which disease(s)? How many persons?" The form is available from https://www.svv.ch/en/insurance/insurance-medicine/services-medical-doctors-and-case-managers (consulted on 30 July 2020).

[8] In many, if not most instances, data about DS2 will also concern DS1. For example, if the individual (DS1) discloses that her mother (DS2) has cancer, this information can be used to draw certain likely conclusions about DS1, mainly her increased risk of cancer, but also the mere existence of a mother-daughter relationship.

[9] In a network (online) perspective, some scientists proposed the following definition of *interdependent privacy:* "[T]he privacy of individual users is bound to be affected by the decisions of others, and could be out of their own control": Biczók G./Chia P. H., *Interdependent Privacy: Let Me Share Your Data,* in: Sadeghi A. R. (eds), *Financial Cryptography and Data Security, Lecture Notes in Computer Science,* Vol. 7859, Springer, Berlin, Heidelberg 2013.

[10] Regarding the issue of interdependent privacy in general: Kamleitner B./Mitchell V., *Your Data Is My Data: A Framework for Adressing Interdependent Privacy Infringements,* in: *Journal of Public Policy & Marketing,* Vol. 38(4), 2019, pp. 433–450; Olteanu A.-M./Huguenin K./Dacosta I./Hubaux J.-P., *Consensual and Privacy-Preserving Sharing of Multi-Subject and Interdependent Data,* École Polytechnique Fédérale de Lausanne 2018; Humbert M./Ayday E./Hubaux J.-P./Telenti A., *Quantifying Interdependent Risks in Genomic Privacy,* in: *ACM Transactions on Privacy and Security,* Vol. 20, No. 1, Article 3, 2017; Humbert M./Trubert B./Huguenin K., *A Survey on Interdependent Privacy,* École Polytechnique Fédérale de Lausanne 2019; Levy K./Schneier B., *Privacy Threats in Intimate Relationships,* in: *Journal of Cybersecurity,* Vol. 6: 1–13, 2020.

[11] The matter addressed in this paper should not be confused with the case of DS1 requested by DS2 to disclose information on the latter in order to ease the creation of a new contractual relationship between DS2 and C1. Regarding the employment contract: Meier P., *Protection des données: Fondements, principes généraux et droit privé,* Berne 2010, pp. 664–668. Regarding the lease contract: Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, pp. 43 ss.

[12] In some "extreme" cases, the penal provisions on defamation, Art. 173 of the Swiss Criminal Code of 21 December 1937 (CC 311.0) and wilful defamation, art. 174 of the Swiss Criminal Code.

[13] Act of 19 June 1992 (CC 235.1). A revised version of the Swiss FADP has been adopted by the Federal Parliament on 25 September 2020, but is not to enter into force until (probably) 2022. The new text is available at FF 2020 7397. See a comparative table between the actual and the future versions of the FADP in: Di Tria L., *La Suisse se dote (enfin) d'une nouvelle Loi fédérale sur la protection des données – Tableau comparatif mis à disposition,* in: www.swissprivacy.law/13, 2020. In this paper, we will refer to the actual version of the FADP. For our purposes, the changes between the actual and the future versions are not significant.

is subject to the FADP, according to Articles 2 and 3 FADP.[14] That the communication is made by an individual (*i. e.,* natural person) is irrelevant.[15] That it is done in the context of personal, work or social relationship is also irrelevant.[16] Article 2.2.a FADP does contain an exception about individuals' use of personal data for personal purposes, but this exception is not available if the personal data is *communicated to a third party.*[17]

Returning to our first example, the patient who is asked about diseases incurred by family members (DS2) is invited to communicate personal data[18] about third parties. Even if she does not mention her mother's name, or perhaps not even saying that it was her mother who suffered from breast cancer, DS2 is in all likelihood identifiable.[19] As a consequence, the patient is obliged to abide by the FADP. The following question is therefore whether the patient is allowed to provide this information, on request or perhaps even voluntarily.[20]

It should be noted at this stage that medical information is always classified as *sensitive* personal data under the FADP (Article 3.c.2 FADP). It is so regardless of whether this piece of medical information could be used to discriminate or stigmatize the individual. Even basic information, such as blood type, is held to be health data.[21] That the medical data concerns DS1, DS2 or both of them (*e. g.,* in the case of genetically inherited disease) is irrelevant.

Under the FADP, processing of personal data requires justification.[22] The most common justification is *consent.*[23] However, only the data subject *directly concerned* can consent. Therefore, DS1 cannot provide consent for (or instead of) DS2, unless of course she is the legal representative of DS2 (as in parent-child relationship). Hence, another justification must be found. Under Article 13 FADP, the patient could claim that her communication is justified by *her own private prevailing interest* in getting optimal medical treatment.[24] Disclosing that her father has heart disease may help her doctor suggest the best course of care for her. Here, the FADP calls for a *balancing exercise* between the interest of the patient (DS1) and the interest of the family members or third parties (DS2) whose privacy is harmed. Since the information is being provided to a health care professional bound by a strict obligation of privacy,[25] one could argue with some justification that the interests of the patient (DS1) must prevail over that of DS2. Moreover, there is a long tradition and therefore long-standing expectations that a medical diagnosis requires information about family members and close contacts (DS2).[26] Although tradition is not by itself a justification, it can be taken into consideration when balancing opposing interests.

The situation is somewhat different in our second hypothesis. The benefit hoped for by the prospective client is *insurance coverage.* At least in Switzerland, this is primarily a financial interest, since basic needs are ordinarily covered by social insurance – insurance for which questions about family members are neither asked nor needed. In addition, private insurance companies are not bound by medical secrecy, but only by ordinary duties of confidentiality stemming from the contract with the client or from the FADP. The outcome of the balancing of interests is thus less obvious in this instance.

In the *research setting,* the research participant (DS1) often has *no personal* interest in disclosing personal data about family members (DS2). She may be participating in a research project solely to advance knowledge in the public interest, without any individual gain. Thus, there is no prevailing private interest of

[14] Regarding the scope of application of the FADP: Préposé fédéral à la protection des données et à la transparence PFPDT, *Guide relatif au traitement des données personnelles dans le domaine medical – Traitement des données personnelles par des personnes privées et des organes fédéraux,* Berne 2002, p. 4; BSK DSG-Maurer-Lambrou/Kunz, art. 2 NN 2–19c.

[15] The Swiss provisions on data protection apply in the same way, regardless of whether the controller is a natural or legal person. The same holds for the provisions on medical secrecy and medical research.

[16] Meier P., *Protection des données: Fondements, principes généraux et droit privé,* Berne 2010, pp. 186–188; In a EU perspective, see the justification in: CJEU, *Arrêt Lindqvist,* C-101/01, ECLI:EU:C:2003:596, § 46 ss.

[17] BSK DSG-Maurer-Lambrou/Kunz, art. 2 N 21.

[18] As per Article 3.a FADP, "The following definitions apply: (a) *personal data (data):* all information relating to an identified or identifiable person".

[19] It is at least so in the family setting. For example, the doctor will ask "Has there been any cancer in your family?". If the patient answers yes, the doctor will almost certainly follow up by asking "Who was it, what kind of cancer, at what age, with what outcome?". Identification may be more difficult when the information disclosed refers to non-family members, for example, sexual partners or casual contacts in the COVID-19 context.

[20] The patient is understandably worried because her two older sisters have recently died from breast cancer and thus breaches the topic on her own.

[21] Since it is classified as sensitive personal data, the protection shall be wider: Fanti S., *Big Data & Protection des données dans le domaine santé,* in: Dominique Sprumont (éd.), *Nouvelles technologies et santé publique,* 22^{e} journée de droit de la santé, Éditions Weblaw, Berne 2016, pp. 77–106; Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, pp. 75–76; Regarding the way people perceive "data on health" and its importance: Tall I., *Le renforcement de la loi fédérale sur la protection des données: le cas de la protection de la vie privée dès la conception (privacy by design),* in: Cahier de l'IDHEAP 289/2015, Lausanne 2015, p. 53.

[22] Articles 4 and 13 FADP.

[23] BSK DSG-Rampini, art. 13 NN 3–14.

[24] BSK DSG-Rampini, art. 13 NN 29–33; Meier P., *Protection des données: Fondements, principes généraux et droit privé,* Berne 2010, pp. 532–557. The criteria used in order to determine the "prevailing character" (Articles 13.1 & 2 FADP) are the same as the ones used to determine the "proportionality" (Article 4.2 FADP): Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, p. 93.

[25] BSK StGB-Oberholzer, art. 321 N 9 (criminal sanctions); BSK DSG-Rampini, art. 15 NN 4–6 (civil liability).

[26] *Cf. supra* fn. 3 to 6.

DS1. A *public interest*[27] in promoting research may come into consideration, however. Indeed, Article 13.2.e FADP states: "[a]n overriding interest of the person processing the data shall in particular be considered if that person: (e) processes personal data for purposes not relating to a specific person, in particular for the purposes of research, planning and statistics and publishes the results in such a manner that the data subjects may not be identified".[28] This last requirement is usually satisfied, since research publications never state names of subjects nor permit their identification.[29]

Still, it may be hard to claim that this public interest of research always prevails over the interest of DS2, especially since the latter may not even be informed of the disclosure. This conclusion is backed by the rule of the Federal Act on Research involving Human Beings (HRA),[30] which nearly always requires the explicit consent of research participants.[31] It would be somewhat odd if the legislature had mandated the prior informed consent of data participants (DS1), but would accept these participants disclosing personal data about third parties (DS2). In our view, research subjects should obtain the agreement of family members about whom they intend to disclose information. Alternatively, a more explicit legal basis in the FADP or in the HRA would be necessary to alter the balance of interests.

III. Request by a Controller to Receive Data About Another Data Subject

We have just examined the extent to which the patient, client or research participant (DS1) herself may communicate information about family members, partners or contact persons (DS2). We now turn to the corresponding question of whether the doctor, insurer or researcher (C1) is *entitled to ask for and then retain such information*.

Under the definition of Article 3.i FADP, C1 is held to be a controller of the data file because C1 "decide[s] on the purpose and content of a data file" containing personal data.[32]

The next issue is whether C1's processing of personal data is licit and justified under Articles 4 and 13 FADP. That C1 receives the personal data about DS2 from DS1 who gave it "freely" (and perhaps even spontaneously) is *no justification in itself*. Each controller subject to the FADP needs her own justification to process personal data from each data subject.

The doctor (C1) in the first hypothesis (medical setting) can reasonably argue that processing of personal data about DS2 is justified by a private prevailing interest, that of her patient (DS1). The same reasons put forward above – *i. e.* finding the right diagnosis and deciding on the best medical course of action for DS1 – also justify the actions of the doctor, in addition to those of the patients. Thus, the doctor *may solicit* the information, but the patient of course remains free to refuse it or even to lie, depending on the *wrongfulness* of the questions.[33] If the information is relevant (*e. g.* when a father and a brother have died of cardiac arrest), it can also be kept in the patient's file, because it may become useful at a later point in time.

Among the interests of the *insurance company,* their private interest in calculating premiums correctly is obviously an important one. Even the Federal Act on Human Genetic Testing (HGTA)[34] recognizes this interest when it allows insurance companies to ask for genetic data *about the* (actual and prospective) *client,* as long as the data at issue is not predictive genetic data[35] (and sometimes even if it is[36]). However, the HGTA does *not address* the genetic privacy of *family members*. The balancing of the interests at issue here is very difficult. On the one hand, clients may want to game the system by securing low insurance coverage when they know they are a "bad risk", based on information they hold about family members. On the other hand, insurance companies have a legitimate interest in preventing such a strategy, because the insurance system is fundamentally based on symmetry of information (both parties are on equal footing with respect

[27] Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, pp. 177–179.

[28] Steinauer P.-H./Fountoulakis C., *Droit des personnes physiques et de la protection de l'adulte,* Berne 2014, p. 306–310; Meier P., *Protection des données: Fondements, principes généraux et droit privé,* Berne 2010, pp. 558–562.

[29] Hertig Pea A., *La protection des données personnelles médicales est-elle efficace? Étude des moyens d'action en droit suisse,* Bâle 2013, p. 151; Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, p. 96.

[30] Act of 30 September 2011 (CC 810.30).

[31] Article 7.1 HRA.

[32] See the case law of the EU Court of Justice: CJEU, *Jehovan todistajat,* C-25/17, ECLI:EU:C:2018:551; CJEU, *Wirtschaftsakademie,* C-210/16, ECLI:EU:C:2018:388; CJEU, *Fashion ID,* C-40/17, ECLI:EU:C:2019:629.

[33] The *right to lie* developed under Swiss labour law in case of prohibited questions asked by an employer to an employee, in violation of Article 328b of the Code of Obligations. Regarding the wrongfulness of the questions: CR CO I-Aubert, art. 328b NN 1–4 & 7. Regarding the "right to lie" of the employee: CR CO I-Aubert, art. 328b NN 5–6.

[34] Act of 8 October 2004 (CC 810.12); A revised version of the Swiss HGTA, which has been adopted on 15 June 2018, will enter into force in 2021. Regarding our topic, there are almost no differences between the two texts. In this paper, we will refer both to the actual and the soon-to-be in force HGTA (hereafter: *n*HGTA).

[35] Article 3.1.g of the Federal Act of 2 April 1908 on Insurance Contracts (CC 221.229.1).

[36] Article 26 HGTA (Article 42 *n*HGTA) forbids insurers from asking for non-predictive genetic data, while Article 27 HGTA (Article 43 *n*HGTA) allows it, as long as the insurance contract doesn't fall under the scope of Article 27.1.a to e HGTA (Article 43.1.a to e *n*HGTA). Regarding these matters, there is no material changes between the HGTA and the *n*HGTA.

to information held).[37] In this case, family members (DS2) incur a severe breach of their privacy, for which they do not give consent and gain nothing. Moreover, as mentioned earlier, the benefit of the insured individual is mainly a financial one.[38] The solution could come from a compromise inspired by the HGTA:[39] above a certain threshold, the information would need to be disclosed; below it would not. Indeed, for predictive (*i. e.* before the onset of symptoms) genetic analysis, private insurance companies are usually allowed to request the client submit all *available* results if the amount at issue exceeds CHF 40000 per year or a lump sum of CHF 400000.[40] When this threshold or a different one (as the balancing of interests would justify) is not reached, the prospective client would have the right to refuse to answer or even lie.[41] If the contract is ultimately not entered into, the information about DS2 should be permanently destroyed, because keeping it in the file is simply disproportionate.

Finally, turning to the *researcher* (C1): A question remains as to whether she can always claim to act in the public interest? We saw above that this is debatable. A different question is whether researchers may avail themselves of Article 34 HRA to process information about DS2 without the latter's consent.[42] Article 34 HRA allows researchers to ask the ethics commission for a consent *waiver, inter alia* when it is impossible to conduct research on the basis of data subjects' consent.[43] Many research projects in Switzerland are accepted on this basis.[44] The waiver covers subject-identified (*i. e.* named) personal data, which is usually transformed at some point into coded data.[45]

To our knowledge, Article 34 ~~HRA~~ has never been applied in situations where the "direct" research subject (DS1) has given consent, but not the "indirect" participants, such as family members (DS2). The provision was meant to apply when *no consent whatsoever* is present. The legislature did not address the possibility that consent waivers could cover only some part of the research. However, given the language of Article 34 HRA and the general principle *"a maiore ad minus"*, this is not excluded. Researchers could therefore pursue this legal pathway. As mentioned above, to our knowledge, this has not yet occured.

Because medical data is sensitive data, C1 has an additional duty: to inform data subjects under Article 14 FADP.[46] This provision *explicitly* applies when C1 has acquired sensitive data *from a third party*. Therefore, C1's processing of personal data about DS2 provided by DS1 is unequivocally within the scope of this provision. Article 14.2 FADP lists which information must be given to DS2 (*e. g.*, identity of the controller, purpose of the processing, further recipients in case of third-party communication). Article 14.3 FADP requires that DS2 be given this information "at the latest when the data is stored or if the data is not stored, on its first disclosure to a third party". Article 14.4.b FADP[47] allows a first exception in two cases, of which one is: "[t]he duty of the controller of the data file to provide information ceases to apply if the data subject has already been informed or, in cases under [14.3 FADP], if: (a) the storage or the disclosure of the data is expressly provided for by law, or (b) the provision of information is *not possible or possible only with disproportionate inconvenience or expense"*.[48] Since C1 is collecting information about DS2 directly from DS1, it is hard to argue that contacting DS2 would be impossible or dispropor-

[37] Of course, it can be argued that, in practice, insurance companies have access to a trove of general statistical data never available to clients. Thus, these companies can *quantify* the risks, whereas the individual can only base her decision to seek and accept insurance based on *her own* medical information (and possibly that of her family).

[38] As mentioned earlier, for most individuals, social mandatory insurance covers the main risks of life. However, for certain people, notably the independent workers, securing private insurance may be essential.

[39] Lehmann A., *Les réserves pour raisons de santé et les conséquences d'une fausse déclaration de santé en droit des assurances,* in: *Haftung und Versicherung,* Lausanne 2017, pp. 153–154; Noventa C., *Genomisierte Prävention in der obligatorischen Krankenpflegeversicherung,* in: *Zeitschrift für Recht und Gesundheit,* Zürich 2014, NN 126–127; Rohmer, S., *Spécificité des données génétiques et protection de la sphere privée: les exemples des profils d'ADN dans la procédure pénale et du diagnostic génétique,* Zürich, 2006, XLVIII, p. 314–315; Sprumont D./Beguin M.-L., *Anamnèse familiale et assurance vie,* Plaidoyer 3/02, pp. 54 ss.

[40] Articles 26 and 27.1.d & e HGTA (Articles 42 and 42.1.d & e *n*HGTA).

[41] In our view, in the hypothesis of an insurance contract negotiation, the concept of the right to lie – and its specific conditions – shall apply *mutatis mutandis* whenever an insurer asks prohibited questions to a prospective client. Articles 6 ss of the Federal Act on Insurance Contracts provide the right, to the insurer, to terminate the contract under some specific conditions (in French *"réticence"*). *«La réticence réside dans une divergence entre la vérité et ce qui a été déclaré (…) il faut que la réponse donnée à la question de l'assureur ne soit pas conforme à la vérité, par omission ou inexactitude»:* ATF 136 III 334, paragraph 2.3. Since the insurer has to evaluate the risks of the client, there is an undeniable obligation of the latter to communicate true and complete information (Articles 4 and 5 of the Federal Act on Insurance Contracts). However, the insurer shall not go further than necessary in questioning the client, *e. g.* by asking illegal questions. Failing to do so, the insurer shall be deprived of his right to terminate the contract.

[42] Regarding the case of a treating doctor gathering information for research purposes and Article 34 HRA: Steinauer P.-H./Fountoulakis C., *Droit des personnes physiques et de la protection de l'adulte,* Berne 2014, p. 319.

[43] SHK-Rudin, art. 34 NN 9–13.

[44] Junod V./Elger B., *Données codées, non-codées ou anonymes: des choix compliqués dans la recherche médicale rétrospective,* in: Jusletter 10 December 2018.

[45] As a reminder, both under HRA and FADP, coded data is viewed as *personal data*~~: *cf. supra* fn. 3~~7.

[46] Métille S., *Internet et droit: Protection de la personnalité et questions pratiques,* in: quid iuris? Band/Nr. 20, Genève 2017, p. 85.

[47] BSK DSG-Rampini/Fuchs, art. 14 NN 16–19.

[48] Our emphasis.

tionate. On the contrary, in many cases, it would be easy and entail only minimal cost. An inconvenience may exist, however, when contacting DS2 would entail a further breach to his privacy, given the need to obtain his or her complete contact details.

A second exception is provided by Article 14.5 FADP:[49] "[t]he controller of the data file may refuse, restrict or defer the provision of information subject to the requirements of Article 9 paragraphs 1 and 4". Under Article 9.1 FADP, "[t]he controller of a data file may refuse, restrict or defer the provision of information where: (a) a formal enactment so provides; [or] (b) this is required to protect the *overriding interests of third parties*".[50] Under Article 9.4 FADP, "[t]he private controller of a data file may further refuse, restrict or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties".[51] In our view, this exception is unlikely to apply. One does not see how *denying* DS2 information would ordinarily *serve an overriding interest*. The doctor's interests are not harmed by giving this information, nor are those of the insurance company or researcher. Similarly, informing DS2 does not harm DS1. We will admit an exception where DS1 and DS2 are at odds (*e.g.* when family members no longer on speaking terms) or where disclosure is likely to cause additional privacy harms (e.g., when disclosure to DS2 will harm DS1's privacy).[52] In some cases, informing DS2 will require first obtaining his contact information, which may cause greater harm to his privacy; this would justify a third exception.[53] Finally, the added administrative burden should not always qualify as an overriding interest to refuse to disclose the information, and should instead be handled on a case-by-case basis.

IV. Controller's Uses Beyond the One Initially Contemplated

As mentioned in the introduction, a doctor, an insurance company or a researcher may be in a situation in which they have a reason or an incentive to use personal data about DS2 (obtained from DS1) for a purpose unrelated to the relationship with DS1. The doctor may want to use it to treat another patient (DS2[54]) belonging to the same family; the insurance company may want to use it to calculate on the premiums of a DS2 client; the researcher may find herself in a position to merge the personal data she acquired on DS2 with other data pertaining to DS2 to extend its project. To simplify the analysis, and as it is most often the case, we assume that neither DS1 nor DS2 are aware of this further use and therefore neither one consented to it.

A general principle of the FADP is that personal data can *only be processed for the stated or recognizable purpose*[55] – according to Articles 4.3: "[p]ersonal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law"[56] and 4.4 FADP: "[t]he collection of personal data and in particular the purpose of its processing must be evident to the data subject".[57] Surprisingly, perhaps, these rules have no exceptions in the FADP, except when the law provides otherwise, usually for the benefit of federal authorities.[58] Hence, if neither DS1 nor DS2 consented to further uses nor were informed of them, the latter uses are normally illegal under the FADP.

Regardless of whether it is the doctor or the insurer, use for a different purpose appears to be prohibited.[59] This may appear somewhat counterintuitive. Indeed, it would be strange for a doctor *not* to use information she holds to save the life of DS2 (even though this is an unlikely scenario[60]) simply because neither DS1 nor DS2 was informed that this personal data could be used to such purpose. In that case, an *"état de nécessité"* (state of necessity) could perhaps be invoked[61]. However, if the information is only "nice to

[49] BSK DSG-Rampini/Fuchs, art. 14 NN 20–24.

[50] Our emphasis.

[51] Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, p. 77.

[52] For example, DS1 participated in a HIV-study in which she had to disclose when and how she was infected; she answered that it was by her mother (DS2) through birth. If the investigator were to contact DS2 to inform her about the disclosure, she would be revealing that DS1 is now HIV positive, a piece of information that DS2 may not have and that DS1 may want to keep confidential.

[53] Taking again our last example (*cf. supra* fn. 52), if the investigator needs the full name, the address and the phone number of DS2 to contact her, this would cause an increased privacy harm.

[54] It could be DS2, but also a DS3. For example, if the patient discloses that her mother has had cancer, the doctor, the insurance or the researcher may use this information in connection with the mother herself, but possibly in connection with other family members, such as a sister.

[55] BSK DSG-Maurer-Lambrou/Steiner, art. 4 NN 3–16e.

[56] Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, pp. 66–67; Steinauer P.-H./Fountoulakis C., *Droit des personnes physiques et de la protection de l'adulte,* Berne 2014, p. 298.

[57] Flueckiger C., *Dopage, santé des sportifs professionnels et protection des données médicales,* in: CERT – Centre d'études des relations du travail Band/Nr. 1, Bâle 2008, pp. 67–68; Steinauer P.-H./Fountoulakis C., *Droit des personnes physiques et de la protection de l'adulte,* Berne 2014, pp. 298–299.

[58] BSK DSG-Maurer-Lambrou/Steiner, art. 4 NN 15 and 16e.

[59] Métille S., *Internet et droit: Protection de la personnalité et questions pratiques,* in: qi? – quid iuris? Band/Nr. 20, Genève 2017, pp. 85–86.

[60] For example, the researcher learns that DS1 is HIV-positive and is having unprotected sex with her partner, while refusing to disclose her status. When would it be licit for the researcher to contact the partner directly?

[61] Article 17 of the Swiss Criminal Code: CR CP II-Chappuis, art. 321 NN 199–122. Regarding *medical data* and Article 6.2.e FADP: Meier P., *Protection des données: Fondements, principes généraux et droit privé,* Berne 2010, pp. 473.

have"[62] (*e. g.* "by the way, a family member of yours is suffering from breast cancer, so you may want to have regular check-ups yourself"), such disclosure remains, in our view, illegal.[63] Deciding where the frontier lays is – of course – far from easy.[64] Such decisions are made all the more challenging by the fact that data controllers must reach each decision independently.

In the context of insurance, exceptions should not be allowed. Indeed, when an insurance company gathers information about a prospective client, it is free to ask this person directly, instead of exploiting information it received through other clients. No urgency *("état de nécessité")* can come into play. It should ask the person directly rather than exploit the information.

Finally, for research, the exception of Article 34 HRA described above may meet the requirements of "provided for by law" in Article 4.3 *in fine* FADP. In other words, it can be argued that if the researcher is relying on a waiver from an ethics commission (*cf.* Article 34 HRA), she may use the information received from DS1 about DS2 for a different research project, bypassing the duty to provide information and the need for consent from both individuals.

V. Further Communication with Third Parties

Finally, we turn to the instances in which C1 communicates information to third parties (C2) who will make their own use of the data, as when, for example, the doctor calls a specialist in oncology to discuss her patient's case in such a way that the identity of DS1 and DS2 can be inferred by this specialist.[65] Other such cases include when the insurance company communicates the personal data about DS1 and DS2 to another company of the group, *e. g.* a different entity offering life insurance, or when researchers in Switzerland team up with other scientists and pool their respective data. In these cases, neither DS1 nor DS2 are informed.

Under Article 12.2.c FADP, sensitive information can only be communicated to third parties with proper justification.[66] Strangely, the justifications contemplated by Article 13.2 FADP are the same as when the data is not sensitive.[67] Hence, consent, prevailing private/public interest or law can be invoked. We can therefore refer to the explanations provided above (*cf.* Section II).

However, in our view, the balancing exercise here is even more delicate.

In the first hypothesis (*i. e.* treatment setting), by consulting a specialist, the physician is helping provide the best possible care for her patient, which is her responsibility both under the law and under the medical care contract.[68] Yet, it is considered proper for C1 to mention this "referral" to her patient (DS1) *beforehand,* and even better to ask for DS1's explicit consent.[69] Most authors commenting on medical secrecy are of the view that discussion between the attending physician and a specialist requires the consent of the patient (DS1), when the identity of the patient can be inferred.[70] The issue of whether DS2 should also consent if her information is disclosed (*e. g.* "I have this 45-year-old patient whom you treated before. Her sister has breast cancer and I am thinking of doing this as a preventive measure, what do you think?") has not been discussed in the legal literature. However, if the consent of the patient is viewed as required, this should *a fortiori* be the case when information is revealed about third parties not contractually bound to the physician.

At this stage, because communication to a third party is taking place, the criminal sanctions for breaches of

[62] Regarding the concept of *"économicité des données"*: Métille S., *Internet et droit: Protection de la personnalité et questions pratiques,* in: qi? – quid iuris? Band/Nr. 20, Genève 2017, pp. 83–83.

[63] Christinat Rachel, *Le procès en responsabilité civile médicale: mise en œuvre en procédures civile et administrative,* in *Collection neuchâteloise* (2019), p. 129.

[64] Usually, the closer the genetic relationship, the more relevant the information. If the patient had a mother and a sister each suffering from breast cancer, she is at much higher risk and the information is much more important than if a far-removed cousin were the only one diagnosed.

[65] A communication made in an anonymous format to the recipient (patient designated as X, with neither name, nor initials, insurance number, address, telephone, email, *etc.*) remains permissible, because it does not fall within the scope of the FADP. The question whether anonymity should be decided based on the perspective of the receiving or communicating party has not been settled under the FADP. However, it makes more sense to decide it using the perspective of the recipient. If the specialist does not know who the treating doctor/primary care doctor/GP is talking about, no privacy threat occurs.

[66] Steinauer P.-H./Fountoulakis C., *Droit des personnes physiques et de la protection de l'adulte,* Berne 2014, pp. 303–304.

[67] BSK DSG-Rampini, art. 12 NN 6–15.

[68] *Cf. supra* fn. 3 to 6.

[69] In practice, the consent is often somewhat implicit, at least not fully informed. Burgat S., *La télémédecine et le droit suisse: Analyse au regard du droit contractuel, de la Loi fédérale sur la protection des données, de la responsabilité civile et des assurances sociales,* in: CN – Collection neuchâteloise, Neuchâtel 2012, pp. 270–286; Regarding the duty to disclose information to a third party, (*e. g.* in case of transmissible diseases): Kuenzi S., *Rapport sur la conférence du Forum Suisse pour le Droit de la Communication sur la protection des données du premier octobre 2004,* in: sic! 3/2005, Zürich 2005; CR CP II-Chappuis, art. 321 N 3 & 123; In case of billing by a third party: Caisse des Médecins, *Extrait du règlement sur le traitement des données,* Urdorf 2018; Regarding the relationship between the insurer and its medical advisor: TAF A-7375/2006.

[70] For billing purposes, the identity of the patient may be necessary: Préposé fédéral à la protection des données et à la transparence PFPDT, *Guide relatif au traitement des données personnelles dans le domaine medical – Traitement des données personnelles par des personnes privées et des organes fédéraux,* Berne 2002, pp. 17 ss; In a cantonal perspective: Article 80 of the Canton de Vaud's Act on Public Health of 29 May 1985 (CCV – 800.01); Article 87 of the Canton de Genève's Act on Health of 7 April 2006 (CCGE – K 1 03).

medical secrecy also come into play. Under Article 321 of the Swiss Criminal Code, a health professional who breaches medical secrecy commits a felony unless specifically authorized (Articles 321.2 & 3)[71]. The objective elements of the offense are met (1) even if the information is not strictly medical in nature, since it is only required that it refers to the health of a person,[72] (2) even when there is no contractual bond between the data subject and the physician[73] (3) and even if the information was not directly provided by the data subject as long as there is information "that has been confided to him [the health professional] in his professional capacity or which has come to his knowledge in the practice of his profession".[74] Therefore, the physician (C1) who communicates information about DS2 to C2 without the consent of DS2, without the authorization of the public authority or without a legal basis requiring the physician to do so, is criminally liable. A similar provision, Article 321bis of the Swiss Criminal Code, applies to medical researchers.

For *insurance companies,* disclosure to third parties[75] should never be allowed without the consent of DS2. There is no prevailing private interest of such companies to allow the bypassing of consent. Moreover, especially during the negotiation, asking DS2's explicit consent is not overly burdensome.

Finally, in the *research hypothesis,* both C1 and C2 could avail themselves – once again – of the exception of Article 34 HRA, provided of course that C1 is willing to provide C2 her information about DS1 and DS2. A research ethics committee can allow access to so-called unconsented data even if it was originally gathered by a different party. The party gathering the data must collaborate in the process. For example, if the CHUV[76] in Lausanne and the HUG[77] in Geneva want to share and merge their personal research data to conduct a joint project, they can submit the project to a leading ethics commission[78] and apply jointly for the Article 34 HRA waiver. If the committee does grant the waiver, the data will be made available to both group of researchers. If the data stored by one hospital includes information disclosed by DS1 about DS2, it will also be made available to the other hospital. In practice, this occurs frequently, as joint research projects are increasingly common to leverage the benefits of large datasets ("Big Data").[79]

VI. Conclusion: Recommendations

A *unique* solution to solve the conflicts among the different stakeholders (DS1, DS2, C1 and C2) does not and cannot exist. Interests at issue are likely to be and to remain opposed. Moreover, only three hypotheses and four issues have been analyzed here. In practice, several other situations may require thorough analysis (*e.g.* genetic analysis for recreational purposes, medical visits for sports purposes, medical data regarding children, prenatal testing, diagnosis for insurance coverage, *etc.*).

Despite the difficulties, our first recommendation would be to add a provision in the FADP that would require a separate balancing of interests whenever more than one data subject's privacy is at issue. Thus, the data subject (DS1) as well as the controllers (C1 and C2) would be obliged to take into account the privacy interest of DS2 when providing, requesting, processing, storing, using and communicating personal data regarding the latter. The doctor would be allowed to seek information about DS2 only if she reached the conclusion that the answers to each specific question were truly helpful.[80] In case of doubt, consent from DS2 should be sought. With on-line tools, blockchain and electronic patient files, obtaining this consent should become easier over time.

[71] Regarding the distinction between the medical secrecy of Article 321 of the Swiss Criminal Code and the duty of discretion of Article 35 FADP: Préposé fédéral à la protection des données et à la transparence PFPDT, *Guide relatif au traitement des données personnelles dans le domaine medical – Traitement des données personnelles par des personnes privées et des organes fédéraux,* Berne 2002, pp. 5–6.

[72] CR CP II-Chappuis, art. 321 N 28.

[73] CR CP II-Chappuis, art. 321 N 44.

[74] CR CP II-Chappuis, art. 321 N 60.

[75] When insurance companies operate in a group structure, disclosure within the entities of the group should be subject to strict limits. This is for example the case when a company offers social sickness insurance and another company of the same group offers complementary sickness insurance. Even when the same companies offer different types of private insurance, transmission of information within the company should not occur unless the client or prospective client has been informed and has agreed beforehand.

[76] Lausanne University Hospital.

[77] Geneva University Hospital.

[78] When a medical research project is taking place across several institutions in different cantons, a lead commission is generally appointed to conduct the main legal, medical and ethical analysis of the project: see Article 27 of the Federal Ordinance of 20 September 2013 on Clinical Trials in Human Research (CC 810.305).

[79] Fanti S., *Big Data & Protection des données dans le domaine santé,* in: Dominique Sprumont (éd.), *Nouvelles technologies et santé publique,* 22^{e} journée de droit de la santé, Éditions Weblaw, Berne 2016, pp. 77–106; Meier P., *Le défi de Big Data dans les relations entre privés: Avec quelques réflexions de lege ferenda,* in: *Forum Europarecht* Band/Nr. 37, Zürich 2016, pp. 47–94; Charlet F., *Réseaux sociaux et protection des données – Analyse des pratiques de Facebook en regard des exigences des droits européens et suisse de la protection des données,* in: *Forum Europarecht* Band/Nr. 39, Zürich 2018, pp. 77–115; Académie Suisse des Sciences Médicales/Fédération des médecins suisses, *Bases juridiques pour le quotidien du médecin: un guide pratique,* 2020, p. 125.

[80] To a reasonable extent, the patient would need to ask herself whether it is necessary to provide information about the diseases suffered by her parents. Of course, in medical settings, patients may find it hard to decide themselves which information is necessary or helpful, as they lack the medical knowledge to conduct such an assessment.

Our second recommendation would be to *set a higher bar in the insurance context*. As mentioned above, a private insurance company should in our view *not* be allowed to ask questions about family members unless the amount to be paid under the future policy reached a certain threshold[81]. This recommendation is inspired by the solution retained for predictive genetic analysis.[82] For example, for a life policy over CHF 400000, the company would be allowed to inquire about the health status of family members – below, it would not. This would provide a balance of interests at stake, since there appears to be a systemic interest when such large amounts are reached. Alternatively or additionally, the law could mandate that DS2 be informed and give her own consent. It would not be unduly difficult for the prospective insurance-taker to have the family member signing a separate form whereby the latter would agree to the disclosure of some of her specific health information.

Our third recommendation would be to facilitate opt-out, or perhaps opt-in, "registers", for research purposes. Opt-out registers are currently being contemplated for organ donations. General opt-in procedures are being tried out for medical research on patients' data (the so-called general consent forms[83] used at an increasingly large number of university hospitals throughout Switzerland[84]). With modern IT tools, it should be possible for a data subject to require heightened privacy protection by signing in to a database.[85] This would encompass the situation of DS2 asking that no data about her be used in research, even if provided voluntarily by DS1. In that case, researchers, and possibly also family members would know that this person is asking for her personal data to be kept strictly confidential, and not be used, for example, for research or other purposes.[86]

We would like to close with some remarks regarding *contact tracing* in the context of the COVID-19 pandemic. It is viewed as sound public health policy to trace individuals who have been in contact with COVID-19-infected persons. The infected persons (here DS1) are asked to disclose the corresponding personal data about DS2 to one or several controllers. When this is done through digital tools (*e. g.* the Bluetooth function of a smartphone having downloaded the corresponding applications[87]), both DS1 and DS2 have consented; the question of whether or not their consent is sufficiently free and informed will be set aside here.

However, when contact tracing is done using traditional means, there is no opportunity for consent, as DS2 is not informed at all, and DS1 is obliged to provide information.[88] Let us take the hypothesis of a politician and his mistress; she receives a COVID-19 positive diagnosis; she (DS1) informs the hospital that she has had close and frequent personal contacts with the politician (DS2), thus breaching his privacy. He then receives a call informing him that he has possibly been exposed to the virus. Because this has occurred during a period of confinement, he can easily guess who this person was,[89] as he has only left his house to see her; this communication

[81] Moreover, it should be proven by the insurer that, at the relevant time (*i. e.* when the questions were asked) DS1 already held the information about DS2. It is not in all cases that an individual is aware of the diseases or disorders suffered by family members. No one should be forced to ask questions about health to family members just in order secure insurance. Moreover, family members should not be forced to provide such information only to help someone obtain insurance coverage.

[82] *Cf. supra* fn. 32 to 34.

[83] It is a standardized form established by the Swiss Academy of Medical Sciences in collaboration with swissethics. The purpose is to facilitate the access to the data of patients treated in hospitals. The form's title is "Information about the use of health-related data and samples for research purposes" and is currently used in the 5 University Hospitals in Switzerland. Other hospitals are invited to implement the form themselves in their organization. The form is available at: https://www.unimedsuisse.ch/fr/projets/consentment-general (consulted on 30 July 2020).

[84] Autorité cantonale de la transparence et de la protection des données du canton de Fribourg, *Rapport d'activité 2018,* Fribourg 2018, pp. 23–24.

[85] An opt-out database exists for example with respect to persons who do not want to receive telemarketing calls; it has not worked very well. Opt-out databases require a secure identification of the users, which entail certain privacy risks.

[86] One problem with such registers is that opt-outs need to be attributed to a given individual who therefore needs to be identified. It is only when the scientists knows that a *named* DS2 does not want her data to be used in research that she can remove the said data.

[87] On SwissCovid, see the various documents from the Swiss Federal Office of Public Health at: https://www.bag.admin.ch/bag/en/home/krankheiten/ausbrueche-epidemien-pandemien/aktuelle-ausbrueche-epidemien/novel-cov/swisscovid-app-und-contact-tracing.html (consulted on 30 July 2020); Vaudenay S./Vuagnoux M., *Analysis of SwissCovid,* EPFL website, at https://infoscience.epfl.ch/record/278048/files/swisscovid.pdf (consulted on 30 July 2020); Dehaye P.-O./Reardon J., *SwissCovid: a critical analysis of risk assessment by Swiss authorities,* Computer Science, Cryptography and Security, 2020, https://arxiv.org/pdf/2006.10719; Legendre F. et al., *Contact tracing: An overview of the Technologies and Cyber Risks,* Computer Science, Cryptography and Security, 2020, https://arxiv.org/abs/2007.02806.

[88] Article 34.2 of the Federal Act of 28 September 2012 on protection against infectious diseases in humans (CC 818.101): Schilter A., *Der Umgang mit gebietsfremden Organismen aus rechtlicher Perspektive,* in: *Schriftenreihe zum Umweltrecht,* Band/Nr. 29, 3. Kapitel: Instrumentarium, 2017, pp. 228–229.

[89] We purposely chose the hypothesis of a person (*in casu* a politician) who did not have to visit his workplace during the mandatory quarantine and assumed that his wife was also confined at home with him.

clearly interferes with the privacy rights of DS2[90]. In case of a politician or other public figure, the privacy and reputational harms could be serious.[91]

However, the disclosure is clearly meant to further public health goals, that is, to minimize the spread of the infection (*e.g.* by mandating quarantine) and to some extent, also to facilitate early medical care for exposed patients. Thus, there is certainly an important public health interest and possibly a relevant private medical interest of DS1. Whether these two interests prevail over the privacy interest of DS2 remains open for discussion and depends on several variables. Mainly, this requires determining *to what extent* allowing for early identification of infected persons and for their possible quarantine saves lives. Reliable answers to this question are unlikely to arise in the short term.

[90] The politician has now to decide: should he decide to take further confinement measures, for example by no longer approaching his wife? Should he tell others he might be infected? Should he get tested? Or instead, can he ignore the information and continue as usual, including getting back to work when the confinement measures are lifted? If he chooses this last option, which he is *prima facie* entitled to do, the breach of privacy will have served no interest, except maybe the autonomy interest of the politician. Of course, not all these issues are directly related to interdependent privacy. Some of them are more closely linked to contagious diseases.

[91] Our example is inspired by what happened in England to a government COVID-19 researcher who then had to resign.