What Will Change at Doctors' Offices with the New DPA? Not Much!

Yaniv Benhamou
Professor, University of Geneva ,
Lawyer Aegis Partners LLC, Geneva

Philipp Fischer
Lawyer, Oberson Abels SA, Geneva

Célian Hirsch
Lawyer, Lecturer at the Universities
of Fribourg and Geneva

Valérie Junod
Professor, Lawyer, Universities of Geneva
and of Lausanne

Deborah Lechtman
Lawyer, CIPP-E & CIP-M, OA Legal, Geneva

Julien Levis
Group Head of Data Privacy, EFG Bank,
Geneva

Keywords: Data Protection, Liability, Physicians in Private Practice

Abstract: In September 2023, the revised Data Protection Act will enter in force. Its objective is to reinforce the rights of individuals whose data are being processed. Physicians will need to ask themselves whether their medical practice complies with the law. Through 11 questions and answers, we deal with the major changes brought by the Act.

Table of Contents

This article is the result of a joint reflection following the AGDA conference in June 2022.

On September 1, 2023, the Data Protection Act (DPA) that we had become accustomed to will be replaced by a new text. The new DPA (nDPA) does not radically change the rules. However, it is stricter, sets out more extensive duties for data controllers (hereinafter abbreviated: DC) and increases the penalties. An overview of its implications is therefore necessary. Here we take the example of a group practice whose healthcare professionals wish to adapt to the new regulation. Through eleven questions, we review the key aspects. The cantonal rules applicable to public hospitals, although broadly similar, are not examined here.

I. Will My Firm Have to Appoint an Independent Data Protection Officer?

No, not necessarily. The data protection officer (DPO) remains optional (art. 10 nDPA). If the firm decides to establish such a function within the meaning of the nDPA, it must however ensure that a truly independent person is identified, which is often difficult in a small practice. The firm may also opt for an external agent, ensuring that the latter has effective access to the personal data processing process to be analyzed.
The creation of this advisory function (i.e. DPO, external or internal) comes with some advantages, but these are tenuous to the point of being negligible. The office may therefore prefer to entrust the tasks related to the nDPA to one or two competent persons with clear specifications, without officially designating them as DPOs.

II. Does My Firm Have to Conduct a Data Protection Impact Assessment (DPIA)?

No. An impact assessment is indeed required "when the envisaged processing is likely to result in a high risk for the personality or fundamental rights" of the individuals concerned (art. 22 para. 1 nDPA). However, an exception is made if the data processing is carried out in order to fulfil a legal obligation (art. 22 para. 4 nDPA). Doctors are obliged to keep written (or digital) medical records of their patients. We can therefore assume that they fall within the scope of this exception.

III. Does My Practice Have to Keep a Register of Data Processing?

Perhaps. Every DC must in principle keep a register of its processing activities that describes how they are carried out (art. 12 nDPA). The document is not necessarily complicated to draw up, but it requires some upstream thinking and analysis to properly understand the life cycle (from collection to destruction) of the data; it must also be kept up to date. An exception is made for companies with less than 250 employees. However, in order to benefit from this exception, the processing activities must also present only "a limited risk of harm to the data subject's personality". Medical practices process medical data, which the regulatory framework describes as "sensitive"; moreover, the loss or unavailability of this data can have serious consequences. Therefore, in our opinion, they may well have to maintain such a register. In any case, beyond the legal obligation to maintain a register, any medical practice would be well advised to identify the processing of personal data that it carries out or that it entrusts to third-party providers.

IV. Does My Practice Need a Written Contract if It Outsources Certain Tasks, Such as Billing?

Not necessarily. The nDPA still does not require a written contract in case of outsourcing, i.e. when the DC (the firm) delegates certain processing (i.e. tasks) of personal data to independent third parties, e.g. agents (art. 9). However, the controller must ensure that the processor complies with both the nDPA and the instructions given by the controller. The controller may be held responsible for any breaches committed by its processor if it has not taken all the necessary measures to prevent them. In such a situation, being able to rely on a written contract detailing the respective obligations is of great help – it allows to prove diligence and good faith. In addition, if the processor is located in a foreign jurisdiction that does not offer an equivalent level of data protection, it becomes necessary to adopt additional safeguards by contract.

V. Does my practice have to have a written patient information policy?

Not necessarily. The principle is that every controller must inform the individuals concerned of how it processes their personal data (art. 19 nDPA). However, art. 20 nDPA introduces an exception that benefits doctors. DC who process data in compliance with a legal obligation are exempt from this obligation. As already mentioned, doctors are required to keep complete medical records, in particular on the basis of cantonal law. However, the exception only covers the maintenance of the medical file, not other "optional" processing such as the outsourcing of certain administrative tasks (e.g. billing). At least for these other tasks, information is needed.

VI. Does My Practice Need to Have a Signed Free and Informed Consent for Each Data Processing?

Not necessarily. The nDPA does not change the rule: as long as the data processing is lawful, there is no need for a justification. In other words, if the firm complies with the DPA, including its general principles (e.g. purpose, proportionality), it is acting lawfully (art. 31 nDPA). However, given the complexity of the rules, it is difficult to assume that all the data processing to be carried out will be lawful. It is therefore in the firm's interest to verify whether each processing operation is covered by a legitimate ground (e.g. a legal obligation). In the absence of a legal obligation, it must establish that it has an overriding private interest in processing the data. Otherwise, it can seek the consent of each individual concerned. However, this third solution is restrictive: it implies, among other things, putting in place a complete and up-to-date information policy (see question V), giving patients the choice to decide, and keeping a record of the consents given; moreover, the consents given can be freely revoked.

VII. A (Former) Patient Requests Full Access to His or Her File, Including Internal Exchanges Between the Treating Physician and Other Specialists. Do I Have to Grant Such Access?

Yes, the practice must respect the patient's right of access (art. 25 ff. nDPA) allowing the patient to ask whether his or her data are processed and to request a copy of the data.

The practice may refuse or restrict the request, in particular if the request for access is made for purposes outside the scope of the DPA (e.g. solely to collect evidence for a future trial or for chicanery reasons). It can also refuse or restrict access if there are

overriding interests; this may sometimes encompass information obtained from third parties (e.g. relatives of the patient) that is in the file and not known to the patient; depending on the case, that information should be carved out.
The right of access is very broad; it extends to notes and documents exchanged between the treating physician and other specialists. Whether it also covers the doctor's internal notes is a delicate matter.

VIII. Can I Collaborate and Communicate with Other Physicians, Including Specialists, as I Have in the Past?

Yes, a physician who needs to discuss the case with another physician (also subject to confidentiality obligation) can continue to do so. This allows to best execute the mandate of care with his or her patient. The patient does not need to give written consent. If the patient's identity is disclosed to the specialist, however, the patient must be informed in advance (except in an emergency, of course).

IX. My Practice Works with Subcontractors Abroad. Are There Any Additional Rules to Be Observed?

If the practice transfers personal data abroad, for example to subcontractors (so-called processors; e.g. cloud storage), it must determine where these companies are located. It should also check which data are accessible to them. To avoid difficulties as much as possible, the medical practice acting as DC will avoid transmitting personal data, for example by sending only encrypted data.
If the subcontractor is located in a country that is deemed to offer adequate data protection, according to the Federal Council's assessment (e.g., member countries of the European Union), then everything is fine – the physicians need not worry further. On the other hand, if the processor is located in a country that is not considered adequate (e.g., the United States), then the trouble begins. The firm will have different options. None of them are ideal, but perhaps the easiest to implement is to obtain patient consent specifically for the outsourcing. Alternatively, the practice will enter into a contract with the said subcontractor that incorporates the model clauses recommended by the Federal Data Protection and Information Commissioner. These clauses are meant to offer additional contractual data safeguards.

X. If Our Practice Has Suffered a Data Leak, Must We Always Inform the Federal Data Protection and Information Commissioner? Or the Persons Affected by the Leak?

Not necessarily. If the firm has lost personal data, if it can no longer access the data (ramson hacking), if the data has been altered (encryption hacking), if it has been made accessible to unauthorized third parties, the firm must consider the impact that the security breach will have on the individuals concerned. If the impact is likely to be serious (high risk to the individual), the DC must inform the Commissioner (art. 24 para. 1 nDPA). If the individuals concerned are in a position to take measures to minimize their risk, the DC must also inform them; the Commissioner may also order that they be informed (art. 24 para. 4 nDPA).
The Federal Commissioner plans to make an ad hoc notification form available on his website. DC should consult this form in advance, so as to react quickly when the time comes.

XI. If We Make a Mistake, Will We Be Penalized?

Yes, potentially. In addition to the possibility for the persons concerned to bring a civil action for damages or compensation for moral prejudice, certain violations of the nDPA are punishable by a fine of a criminal nature. The amount of the fine is relatively high, up to CHF 250,000 (art. 60 to 63). In principle, the fine will be imposed on one or more individuals (as opposed to a legal entity), i.e. the physicians or their assistants. In certain (a priori limited) cases, the fine may be imputed to the company. In order for a criminal sanction to be imposed, the Public Prosecutor's Office must establish that the individual prosecuted acted intentionally, or at least had foreseen that the violation of the nDPA would occur and had accepted the risk. In addition, the victim must have filed a criminal complaint within three months of becoming aware of the violation. Finally, not all violations of the nDPA are subject to a criminal fine, but only the most serious ones or those most precisely defined in articles 60 ff.

The nDPA has not yet come into force and is already causing concern. The principles – as opposed to specific rules – that it establishes are very broad in scope, but also very vague. For example, how will privacy by default and privacy by design be implemented? There are therefore a multitude of questions for which the answers will only become known over time.