BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 8, Number 2 February 2008

Commentary

Legislation and Guidance

Personal Data

News

Legislation and Guidance

Personal Data

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A.

Personal Data

Use and transfer of medical and clinical data in Greece

By Mark E. Schreiber[1], Edwards Angell Palmer & Dodge LLP, 111 Huntington Avenue, Boston, MA 02199. Tel: 617 239.0585; Fax 617.227.4420; mschreiber@eapdlaw.com; and

Nassos Felonis[2],LL.M., M.C.J.& LL.B, deputy managing partner, Bahas, Gramatidis & Partners, Bahas, Gramatidis, Felonis, Emvalomenos, Alexandris, Hadjis – Lawyers Company, 26 Filellinon Street, Athens 10558, Greece. Tel. (+30 210) 33.18.170; Fax (+30 210) 33.18.171; nassos.felonis@bahagram.com

Introduction and Greek legislative framework

As clinical trials, drug development, collaboration, licensing arrangements and pharmacovigilance expands in Greece, data protection issues will increase in importance. An enhanced understanding of the Greek data protection framework will be necessary, particularly as respects collection and transfer abroad of medical and clinical data stored or originating in Greece. Clinical trial researchers, sponsors and others will want to be aware of and ensure that appropriate precautions have been observed and that use of the data is permitted.

Greece, like other E.U./E.E.A. countries, has enacted a data protection law, which covers, among other things, medical information.[3] The Greek data protection law (the "DP Law") established the independent Hellenic "Personal Data Protection Authority" ("PDPA"), which is vested with statutory and regulatory powers to implement and supervise the application of the DP Law.

The transfer of personal information – such as a person's name, address, age, income, health, race, ethnicity or religious beliefs – from Greece (and other European countries) to a recipient located in the U.S. is restricted. Generally speaking, a transfer is only permissible, if (i) the individual (explicitly or implicitly) consents to such transfer, usually in writing, (ii) there is an agreement in place between the recipient in the U.S. and the individual or entity which collected the information in Greece, (such as an E.U. model clause data transfer agreement), or (iii) the U.S. recipient joined the so-called Safe Harbor framework. See below (Section 5 'Cross-border transfer of medical and clinical data', pp. 5–7 of this paper) for a description of transfer conditions and restrictions.

Collection and use of health data

The DP Law follows the structure of the E.U. Directive, and in Article 2 makes the distinction between "personal/simple data" and "sensitive data."

Personal data which reveals information about "*health*" is classified as sensitive data.[4] The term "*health*" in the DP Law includes any information that relates to the biological existence and the mental health of a person. Therefore, according to this definition, sensitive data is any data which reveals information about the physical and mental condition of a person, his/her deficiencies and disabilities, dietary or other relevant needs and the medical record of a patient. The term "*health data*" includes all *medical data*[5] of a person in the broad meaning of the term, including information on prescriptions, drug taking and use of narcotics, (but not their supply when it is not done for the person's own use) and also the wider category of *genetic data*, primarily hereditary characteristics and genetic code[6].

Ambiguity prevails over the classification of "*biometric data*", *i.e.*, bodily characteristics such as skin, eye iris, fingerprint, face characteristics, and "behavioural characteristics" such as voice, lip movement, signature, *etc*. The PDPA seems to consider these as "simple data" (Ruling 245/2000); however, if such biometric data lead to revealing racial characteristics (*e.g.*, skin colour) or the genetic code, then they are classified as "sensitive data." Lastly, a special category of medical data has been established by Law 2737/1999 on "human organ transplants." In Article 9, this law classifies as sensitive data the contents of the National Records for donors and the recipients.

In order to better understand how medical information can be used and/or transferred from a physician or facility in Greece to one in the U.S., important terms are defined in the Act:

- Personal Data: Any information identifying a data subject. General information of statistical nature that cannot be associated with a data subject is not considered personal data.
- Data Subject: The natural person to whom the data refer and whose identity is known or can be ascertained.
- Sensitive Data: Information referring to race or ethnic origin, political idea, religious or philosophical beliefs, ... *health*, social welfare and sex life.
- The processing of sensitive data is prohibited, unless the data subject gave his or her written consent or an exception applies, as it does, for instance, for doctors under certain circumstances.
- Processing: Any activity or series of activities regarding personal data performed ... with or without automated means, such as obtaining, registering, cataloguing, maintaining, storing, using, transferring, disseminating, making available in any other forms, ... deleting or destroying personal data.

Health data processing

The DP Law in Article 7 sets forth a general rule: "the collection and processing of sensitive data is prohibited." However, there are certain exceptions to this general rule, in which sensitive data collection and processing is allowed, following a permit by the PDPA (given for a fixed period, but it may be renewed). "*Health data*" is included in these exceptions.[7]

According to the DP Law (Article 7, para. 2(d)), processing of health data is allowed only if it is performed by a person whose profession is the provision of health services and it is subject to a confidentiality duty or to relevant professional codes (Laws 1565/1939 and 25.5/6.7.1955, and Article 371 of the Penal Code on the "professional confidentiality duty"), and on the further condition that the processing is necessary for medical prevention, diagnosis, treatment or the management of health services. If any of these conditions is missing, then the general prohibition rule applies.[8] However, if the subject grants his/her written consent or the processing is necessary to protect a vital interest of the subject, or if he/she is in a state of physical or legal incapacity, then the exception to the rule would apply (Article 7, para. 2 (a) and (b)).

Another exception refers to processing done exclusively for research and scientific purposes and on the condition that anonymity is observed and all necessary measures are taken for the protection of the interests of the persons concerned (Article 7, para. 2 (f)). This clearly permits clinical trials.

Under the DP Law, any person processing personal data must, unless an exception applies:

- register itself with the PDPA and provide certain information (Article 6 para. 2);
- apply for a permission to process sensitive data (Article 7 para. 2); and
- apply for a permission to transfer personal data to the U.S. (Article 7).

A permit from the PDPA may be issued if adequate protective or security provisions are included. However, Greek physicians are not required to register with the PDPA and can obtain and use personal medical information without a permit, as long as:

- they are subject to the doctor-patient confidentiality rules and/or professional code secrecy rules (Article 7A para. 1 (d))[9];
- they do not disclose such information to third parties (Article 7A para. 1 (d)); and
- the sensitive data is necessary for purposes of preventive medicine, medical diagnosis, or the provision of care or treatment. (Article 7 para. 2 (d)).

A Greek physician can therefore obtain and use personal health information without registration for these purposes. It appears, however, that specific consent may be required from a patient to the extent the physician discloses sensitive data to a doctor in the U.S., even for the above listed purposes.

The DP Law does not specifically address the issue of disclosure of sensitive data at a medical conference or in a journal, but it appears that to the extent that the patient is or can be identified (name, address, picture, specific information as to the medical history), the patient consent must first be obtained. The picture of a lesion on a patient's face may be enough to identify the patient; a radiograph with patient identifiers may likewise identify the patient.

Territorial application generally

The DP Law in Article 3, para. 3, sets the rules that determine the scope of its territorial application, using as a criterion the *place of establishment* of the "*responsible for processing*"[10] entity (or data controller) and the "*performer of processing*"[11] (or data processor) of the *subjects* (persons) to whom the data relates and of the *means* by which the processing is performed:

a. The DP Law applies to processing of personal data, irrespective of the place of residence of the subjects of the data, if the data controller or the data processor is established[12] within the Greek territory or in a place where according to public international law, Greek law would be applicable (Article 3 para. 3 (a)).
b. The DP Law will apply to processing done by a data controller not established in any E.U. country, but in a third country (like the U.S.A.), and that in processing personal data resorts to means (automated or not), located within the Greek territory. An exception to this is provided in the DP Law, in case such means are only used for the purpose of transit through the Greek territory[13] (Article 3, para. 3 (b)).

In such a case, the data controller is obligated to designate a representative established within the Greek territory by a written submission to the PDPA. This person or entity is thus substituted in his rights and obligations; however, the former still remains responsible under the DP Law.

Cross-border transfer of medical and clinical data

The DP Law reflects the E.U. principle of the free transfer of personal data within the E.U. countries. (Article 9). The DP Law only permits the transfer of personal data to the U.S. under limited circumstances, such as if the patient consents to the transfer.[14] There is no general exemption for the transfer of medical information from a Greek doctor to one in the U.S. for medical purposes. However, a lawyer from the PDPA indicated that the transfer via phone or during a conversation does not require a permit, while all other transfers, such as sending medical records, would require such a permit.

Clinical data can be sent abroad if the Greek entity maintains the codes and names, the data sent is anonymous, and there are adequate security measure to prevent disclosure to third parties. On some occasions, however, clinical researchers, trial sponsors and physicians will want access to "good outcome" and "bad outcome" clinical results. This in turn often requires re-identification of the previously anonymised data and thus subjects the transfer to data protection protocols.

Based on conversations with a lawyer from the PDPA, it is our understanding that the requirements for disclosing/transferring medical information from a Greek

  WDPR ISSN 1473-3579

doctor to one in the U.S. (regardless of where the disclosure/transfer occurs) can be summarised as follows:

For purposes of preventive medicine, medical diagnosis, the provision of care or treatment (assuming data is not anonymised)		
	From Physician to Physician or health care facility	*From Physician to Other Third Party, such as Biotech or Pharma company*
By telephone (*i.e.*, from physician to physician)	No registration required No permit required for processing and disclosure/transfer abroad No additional consent of patient likely for processing and transfer abroad (*i.e*, to US)	Registration required Permit required for processing and disclosure/transfer abroad Consent of patient required for processing and disclosure/transfer abroad (*i.e.*, to US)
By mail, fax, email or other electronic means	No registration required No permit required for processing Permit required for disclosure/transfer abroad (*i.e*, to US) Consent of patient likely not required for processing, but required for disclosure/transfer abroad (*i.e*, to US)	Registration required Permit required for processing and disclosure/transfer abroad Consent of patient required for processing and disclosure/transfer abroad (*i.e*, to US)

For other purposes than preventive medicine, medical diagnosis, the provision of care or treatment (assuming data is not anonymised)		
	From Physician to Physician or health care facility	*From Physician to Other Third Party, such as Biotech or Pharma company*
By telephone, mail, fax, e-mail or other electronic means (*i.e.*, from physician to physician)	Registration required Permit required for processing and disclosure/transfer abroad (*i.e*, to US) Consent of patient required for processing and disclosure/transfer abroad (*i.e*, to US)	Registration required Permit required for processing and disclosure/transfer abroad (*i.e*, to US) Consent of patient required for processing and disclosure/transfer abroad (*i.e*, to US)

As regards non-E.U. countries, the DP Law makes a distinction between countries that are considered to provide a satisfactory level of protection for the transferred personal data and those that do not provide such level of protection.[15] The prior permit of the PDPA is required in both cases.

Conclusion

As clinical trials, drug development, related consulting and medical collaborations expand, including in Greece, these data protection rules will need to be applied. Physicians, pharma and biotech companies in Greece will have to have their compliance regimes encompass these data protection protocols. Licensing and partnership agreements will increasingly reflect these obligations. New questions as to applicability, unresolved areas and compliance mechanics are sure to follow in Greece, and the PDPA may need to be further consulted.

1 Attorney Mark E. Schreiber is a partner in Edwards Angell Palmer and Dodge LLP in its Boston office, *www.eapdlaw.com* and Co-Chair for Privacy Matters of the World Law Group, *www.theworldlawgroup.com*, an international affiliation of large law firms. He was a speaker at the 2005 Kytherian Days Conference and this paper updates that previously presented there.

2 Attorney Nassos Felonis is the deputy managing partner of Bahas, Gramatidis & Partners, which is the Greek law firm representative in the World Law Group.

3 'Greek Law on the Protection of Individuals with regard to the Processing of Personal Data,' Law 2472/1997. The Greek Constitution (as recently revised in 2001) in its section of civil rights, contains provisions for the protection of personal and family privacy ("inviolable rights"). As regards "personal data," Article 9A specifically provides that "every person has the right to be protected from the collection, processing and use, especially by electronic means, of his/her personal data. Such protection is to be secured by an independent Authority. All particulars shall be provided in a specific law." In parallel, Directive 95/46/EU of October 24, 1995 provided for such personal data protection and the free circulation of such data within the E.U. countries. As a result, the Greek Government was at the time under a "dual obligation" to enact the specific law to regulate all such matters. Law 2472/1997 was enacted and published in Government Gazette Issue No. 50/A"/10.04.1997. This basic law has been amended by Law 3471/2006 and more recently again by law 3625/2007.

4 "Sensitive data" is that which relates to "racial or ethnic origin, political opinions, religious or philosophical beliefs, membership to a trade-union, *health*, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas" (revised definition pursuant to Article 18, paras. 1 and 2 of new Law 3471/2006).

5 Indicatively see Ruling 15/2006 of PDPA.

6 Article 5.5 of the Constitution expressly protects the "genetic code." The PDPA in its Ruling 115/2001 has held that it is absolutely prohibited to process such data within the context of employment ("supersensitive data"). Also, in its Ruling 15/2001, the PDPA had set a series of strict conditions for the use of genetic data (DNA) for criminal investigations. However, recent amendment by Law 3625/2007 has excluded from the DP Law's scope of application personal and sensitive data, gathered by judicial authorities for the purpose of verification of crimes.

7 On this point it has to be noted that Law 2472/1997 (art. 3) as recently amended by Law 3625/2007, excludes in general from its scope of protection all personal and sensitive data gathered by judicial authorities for the purpose of verification of crimes.

8 The significance of this provision is mainly limited for hospitals, clinics, healthcare facilities, *etc.*, since the DP Law itself (Article 7A) has exempted doctors, nurses, pharmacists, etc. from the obligation to obtain a PDPA permit, on the condition that the processing relates only to medical data (and not health data in general, *e.g.*, genetic data) and such data is not transferred or released to third parties.

9 On this matter see Ruling 60/2005 of the PDPA, which has held that physiotherapists are not exempted from the registration/permit requirement, because their code of ethics did not provide in a legally-binding way for a professional secrecy duty.

10 The "Responsible for Processing" or data controller is the natural person or legal entity, public authority or service or any other organisation, which determines the objective and the method of processing of personal data (Article 2(g)).

11 The "Performer of Processing" or data processor is anyone (as defined above) who process personal data on account of the Responsible for Processing (Article 2 (h)).

12 "Establishment" means real/actual performance of activity within the territory through a permanent presence, whether a branch or subsidiary company (E.U. Directive, Article 19).

13 This exception is in compliance with the principle of free circulation of personal data within the E.U. countries, as provided in the E.U. Directive (Article 4, para. 1 (c)).

14 By definition, all E.U. countries are considered to provide a satisfactory level of protection for personal data. It should be clarified however, that the free circulation of personal data at E.U. level does not negate the required compliance with the particular obligations and restrictions provided in the Greek legislation on collecting and processing personal data (simple and/or sensitive).

15 The criteria considered in order to classify a country as providing such satisfactory level of protection are mainly the nature of personal data, the purpose and the duration of processing, the legislative and regulatory framework of the country concerned, the professional codes, the security/safety measures for the protection of personal data, as well as the level of such protection. As such, only a limited number of countries have been considered by the E.C. as having adequate protections, including Guernsey, Argentina, Canada, Hungary, Switzerland and the Isle of Man. Regarding the U.S., following a dialogue between the U.S. Federal Trade Commission and the European Union, an agreement was reached called "safe harbour arrangement", in order to allow the free flow of data to the U.S. while observing the E.U. regulations. Pursuant to this arrangement, the U.S. Dept. of Commerce established a list of companies that accept the principles of "safe harbour" and maintain a minimum of data protection rules and respective monitoring mechanisms. The European Commission considers participation in this program (and enrolment on this list) as a presumption of a "satisfactory level of protection" for the purposes of cross-border flow of data to the U.S.

In the second category of countries (*i.e.*, those that are considered as not providing such level of protection), the PDPA as a rule is reluctant to grant its permit. In such cases, cross-border transfer is only allowed in exceptional cases and the PDPA will grant its permit only if a limited number of conditions is concurrent, such as the consent of the person concerned; whether the transfer is necessary for protecting a vital interest of the person or for the entering into and performance of a contract between such person and the data controller and/or between a third party for the interests of the subject (in case he/she is in a state of physical or legal inability to provide his/her consent) or for executing pre-contractual measures; whether the transfer is necessary for handling an exceptional need and protecting a higher public interest; whether the transfer is necessary for exercising legal rights before a court; and whether the transfer is made out of a public record which according to the law is accessible by any interested party.

  WDPR ISSN 1473-3579