COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 29 September 2015

T-PD-BUR(2015)06

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD-BUR)

Preliminary draft Recommendation on the protection of health data

The present document contains a draft recommendation prepared by the expert Jeanne Bossi Malafosse on the basis of her report T-PD(2015)07 and taking into account comments made by delegations at the 32nd Plenary Meeting T-PD (1-3 July 2015).

Directorate General Human Rights and Rule of Law

Explanatory memorandum

Chapter I
General provisions

Chapter II
The legal conditions for use of health data

Chapter III
Health data management procedures

Chapter IV
The rights of the individual

Explanatory memorandum

A dramatic progression in the processing of health data has been observed since the adoption of Recommendation No. R (97) 5 on the protection of medical data. It is due to the phenomenon of data virtualisation made possible by the computerisation of the health sector, and to the proliferation of exchanges arising from the development of the Internet.

Growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research, to health system management, and also the increasing involvement of patients, are noteworthy characteristics of this new environment.

Besides, mobility phenomena and the development of connected medical objects and devices contribute to new uses and to the production of a rapidly growing volume of data.

For all these reasons, the more general term “health data” will be preferred to the previously used term “medical data”, deemed to be produced by health professionals.

Health data thus represent unique interests and a potential for creating value, the attainment of which will depend on the ability of countries to organise the development of an ecosystem facilitating their use while guaranteeing respect for privacy and confidentiality of personal data.

States in fact face major challenges today, for which health data processing can and already does perform an essential role. These challenges relate to public health, to the quality of care, medical transparency and democracy, efficiency of the health system in a context of growing health expenditure, as well as to innovation and growth in such varied and important fields as personalised medicine and information technologies.

E-health, that is use of information and communication technologies in the health sector, presents itself as a powerful impetus for quality, safety and efficiency of care, clearly identified by the public authorities. Information systems and digital technologies in general already constitute one of the principal vehicles for improving the quality, organisation and efficiency of our health system.

This assessment shared by the member states prompts a proposal for a new formulation of Recommendation No. R (97) 5 on the protection of medical data along the following lines, while reaffirming the sensitivity of health data and the importance of regulating their use so as to guarantee use in accordance with the rights and fundamental freedoms of the individual, the right to privacy in particular.

Health data should be defined more broadly so that the information characterising a person’s health situation as a whole is also afforded appropriate protection; health provision for patients is henceforth more comprehensive and must take account of a medical and social welfare dimension throughout their course of treatment.

Aware that owing to these developments, the patient’s role has become more important in the management of his own health data, and that new rights are regularly secured to him, it is expedient to take account of them and to make sure that health information systems are deployed in compliance with rules permitting secure exchange and sharing of information and respect for the protection of personal data.

Chapter I
General provisions

1. Purpose (of the draft Recommendation)

This recommendation has the purpose of providing member states with directions for regulating the use of health data in order to guarantee use in accordance with the rights and fundamental freedoms of the individual, particularly the right to privacy. It also provides guidelines for developing interoperable, secured information systems in a manner allowing the quality of care and the efficiency of health systems to be enhanced.

2. Scope (of the draft Recommendation)

This recommendation is applicable to the collection and automatic processing of personal health data, unless domestic law, in a specific context outside the health care and medical welfare sector, provides other appropriate safeguards.

This recommendation also has the purpose of laying down the principles of health data exchange and sharing assisted by digital tools which uphold the rights of the individual and the confidentiality of data.

3. Definitions

For the purposes of this recommendation, the expressions below are defined as follows.

- The expression "personal health data" covers all data that may reveal the data subject's state of health. Replacing the concept of "medical data" by that of "health data" makes it possible not to be restricted only to data produced by health professionals or to the sole indication of an illness, considering that a person's health care also entails knowledge of his/her family situation or social situation and the action of multiple players, particularly health professionals, welfare staff and the person himself.

Explanatory note: The personal health data item – understood as any data item allowing an individual to be identified directly or indirectly – therefore covers, in particular, all information produced by a person or a technical mechanism such as a medical device or a diagnostic apparatus for example, and concerning the person's state of health. Such data may be very different in nature, whether collected during a medical examination, biological samples and genome data included, all medical information about an illness, a disability, a risk of illness, a pharmaceutical treatment, a physiological condition or a biomedical particular, etc., of the data subject, irrespective of its source.

Medical welfare data denotes any data item which is produced by professionals practicing in the social and medical welfare sector and helps to characterise the data subject's state of health and the conditions of his/her health care. For the sake of simplification, the term personal health data also takes in that of medical welfare data.

- The concepts of "anonymisation" and "pseudonymisation" are defined as follows. Anonymisation is the outcome of processing personal data so as to prevent, irreversibly, all identification of the data subject. It is a further stage of personal data processing. Pseudonymisation consists in replacing an identifier (or more generally, personal data) by a pseudonym. This technique may be deemed irreversible or on the other hand may allow the lifting of anonymity (re-identification).
Using even an irreversible pseudonym may facilitate search for correlations between different data sources concerning the same individual and thus increase the risk of re-identification.

The notion of personal data (and thus of anonymous data) is a complex one as there are an increasing number of ways to identify persons. The genuinely anonymous character of individual data should rather be assessed in terms of evaluating the risk of re-identification having regard to multiple

criteria. The borderline between anonymous data and pseudonymised data is not always simple to define and should be consistent with good practice reference frameworks reflecting the state of the art.

Explanatory note: The proliferation of data from different sources relating to one individual, and the new capabilities for processing these data, especially “data matching”, considerably alter the concept of reversibility of the anonymisation of personal data (re-identification). Data considered anonymous at a given time may later pose a high risk of re-identification owing to the appearance of new techniques or of new data sources. The safest anonymisation techniques remain data aggregation transforming individual data into collective data. But these techniques preclude many subsequent processing operations. Thus it is often justifiable to preserve the individuality of data while containing the risk of re-identification of the subjects.
Anonymisation (an irreversible action) remains desirable wherever it is possible, and results in impersonal data. In all other cases, individual data must be considered pseudonymised (or indirectly name-specific) and pose a relatively high risk of re-identification on the one hand and of disclosure on the other. Appropriate security measures should result from evaluation of these two risks (re-identification and disclosure) having regard to the sensitivity of the data processed.

But in relation to personal data protection, pseudonymised data remain personal data.

-The notions of exchanging and sharing personal health data are defined as follows. Data exchange corresponds to communication of information to a clearly identified recipient or recipients by a known transmitting party. Data sharing allows data to be placed at the disposal of several persons entitled to disclosure according to the principles of right of access, without these persons necessarily being known at the outset. The principle of a shared medical record meets this definition.

Chapter II
The legal conditions for use of health data

Principle 1 Compliance with the principles of personal data protection

Personal health data are sensitive data which can only be processed in cases determined by domestic law and at all events in a manner respecting professional secrecy and the privacy of individuals.

Explanatory note:
Compliance with the principles of personal data protection

Definite, lawful and legitimate purpose of processing, relevant data, limited data retention time, application of security measures such as to guarantee the confidentiality of the data and respect for the right of persons and for their information.

The conditions under which health data are used must also be taken into account in order to permit appropriate processing of these data.

Personal health data may accordingly be processed for the following purposes and in accordance with appropriate safeguards provided by domestic law:

i. for preventive medical purposes and for purposes of medical diagnoses, administration of care or treatment, or management of health services by health professionals and those of the social and medical welfare sector;

ii. for purposes of safeguarding the subject’s vital interests or where the subject has plainly made public the information concerning him/her;

ii. for reasons of collective interest in the public health field;

iii. for reasons of collective interest in the field of managing claims for social protection and

health insurance benefits and services;

iv. for reasons relating to research in the field of health and the medical welfare sector;

v. for reasons essential to the recognition, exercise or defence of a right at law;

vi. for statistical, historical or scientific processing operations under the conditions defined by domestic law;

vii. for purposes not specified at the time of collection of the data, when these are lawful, legitimate and involve processing operations which do not interfere with the interests of persons.

They may also be processed for any purpose whatsoever if the data subject or his/her legal representative has explicitly consented, and in accordance with appropriate safeguards provided by domestic law.

The applications which manage personal health data must incorporate the principles of personal data protection and ensure the compliance of their processing with these principles.

Principle 2 Shared medical secrecy for purposes of providing and administering care

Everyone whose health data are used for the aforementioned purposes is entitled to respect for their privacy and to secrecy of their information.

The need for greater co-ordination between professionals operating in the health and social and medical welfare sector should induce the domestic law of each member state to recognise professional secrecy shared between professionals, themselves bound by professional secrecy and participating in the care of the data subject.

Under these conditions, receipt of the subject's consent is not stipulated, prior information being sufficient provided that the subject retains the possibility of objecting at any time to the use and sharing of his/her data.

Professionals not directly involved in the data subject's health care may selectively access personal health data in accordance with professional secrecy and in the cases prescribed by domestic law.

Chapter III
Health data management procedures

The information systems necessary for the processing of personal health data must, from their design onwards, incorporate compliance with reference frameworks and standards such as to render them compliant with the principles of data protection, interoperable, and secured.

Explanatory note: the principle of *privacy by design*

Principle 1 Urbanisation of information systems: definition of a new information technology environment

The evolution of health information technology results in growing interconnection of information systems. These interconnections, in order to comply with the principles of data protection, must comply with the "urbanisation" rules. These rules and reference frameworks are necessary for the development of e-health and are reflected in the adoption of necessary fundamentals for exchange and sharing of personal health data in accordance with the regulations and the principles governing personal data protection.

These rules and reference frameworks must cover the following fields.

i. reliable identification of persons to ensure the uniqueness of their identity within the different information systems. The identifier chosen must be single, unequivocal, lasting and

recognised by all players, and founded on a reliable certification mechanism.

ii. authentication of the persons and systems involved in the processing of the data (reference data considered reliable, revocable and accessible).

iii. use of solutions which are technically and semantically interoperable, founded on common nomenclatures.

iv. use of solutions secured by such means as to guarantee the availability, integrity, confidentiality and auditability of personal health data. In particular, domestic law must make provision for organising and regulating health data collection, retention and restitution procedures.

Means of identification and authentication must be placed at the operatives' disposal to permit secured exchange and sharing procedures.

Domestic law must recognise the legal effectiveness of certain reference frameworks apt to guarantee the interoperability of information systems allowing the processing of personal health data and their recognition by the whole community of operatives, especially when fundamental rights of persons, such as equal access to good quality care, depend on it.

Explanatory note: Soft law/codes of conduct

Explanatory note: interoperability of information systems

Interoperability constitutes the foundation of information exchange between operatives: indeed, it is conducive to the implementation of standardised services between different information systems, in particular virtualised data sharing and exchange services. Interoperability of information systems, on which depend the sharing and exchange of health data, has become a major concern, just as it may command access to and quality of care and represent, in the event of breakdown, a loss of opportunity for patients.

The conditions of interoperability defined by domestic law must meet the requirements of security and confidentiality of personal health data and of individual rights.
This reference framework specifies the standards to be applied in exchanges and when health data are shared between health information systems.

Technical interoperability specifies the protocols for interconnection and information delivery, and the data sharing and exchange services.

Semantic interoperability concerns the syntax and semantics of the health data exchanged or shared. It should allow, in particular, automatic processing of the data within the application programmes.

Principle 2 Health data management services

Each member state should establish services for the exchange and sharing of health data as useful aids especially to the co-ordination of care, complying with security and interoperability reference frameworks.

Since these capabilities for exchange and sharing contribute to the quality of provision as also to the proper management of health systems as well as other goals, for the benefit both of individuals and of the collective interest and public health, professionals in the health and social and medical welfare sector should each be equipped for the virtual management of their activity, enabling them to exchange or share personal health data.

Chapter IV
The rights of the individual

Principe 1 Right to information

Everyone must be informed of the collection and processing of their personal health data.

They must be informed of:

i. the identity and contact details of the person collecting the data,
ii. the purpose for which the data are collected,
iii. the recipients of the data, and planned data transfers to a third country,
iv. the possibility of their data being subsequently processed for a different and unforeseen purpose, in accordance with appropriate safeguards,
v. the conditions and the means made available to them for accessing their health data,
vi. the specific techniques used for collecting, processing and storing their health data.

Everyone must also retain the possibility of objecting, on legitimate grounds, to the processing of their health data. Exceptions may be prescribed by member states' domestic legislation insofar as justified by another legitimate interest such as protection of the data subject's vital interests or having regard to state of health and ability to understand.

In urgent cases and where it is impossible to inform the individual, this obligation to inform may be waived. A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where third parties run a risk of transmission.

Domestic law should provide for appropriate safeguards of a kind ensuring respect for these rights.

Principle 2 Right of access, objection and portability

Everyone must be able to secure access to their personal health data directly from whoever holds them.

The right of access, embodying the right to communication of information on paper as well, enables the data subject to exercise his/her right of rectification and deletion.

It embodies the right to receive the data in a structured format allowing transmission of the data to another controller designated by the data subject.

The right of deletion is exercised with due regard to the cases prescribed by domestic law invoking legitimate grounds.

The data subject is entitled to object on legitimate grounds to the collection of his/her personal health data except where the person holding the data invokes an overriding and legitimate reason concerning the collective interest of public health.

Principle 3 Receipt of consent

Consent to care is an essential right of the individual, subject to the exceptional cases prescribed by domestic law.

The receipt of consent to the collection and processing of health data should be the signification of the data subject's agreement to the use, sharing and exchange of his/her health data under guaranteed conditions of security, provided that clear information is given beforehand.

The cases where consent is stipulated are prescribed by domestic law. Its stipulation should remain compatible with the functioning of the health data management services and with the rules instituting shared medical secrecy for the purposes of providing and administering care.

It must be explicit, clear, unequivocal and unambiguous. Its receipt, where electronic, must be tagged. It does not absolve the person receiving it of his/her obligations to give prior information.