*The New Navigators: from Professionals to Patients*
*R. Baud et al. (Eds.)*
*IOS Press, 2003*



# Law and standards faced to market rules in health information security

**F.A. Allaert[a] , G. Le Teuff[b], C. Quantin[c]**

*[a]Dpt public health and epidemiology MacGill University Montreal Past Chairman CEN TC 251 WG III, "security, safety and quality of healthcare information",*
*[b]Centre d'Evaluation CHRU Dijon,*
*[c]DIM CHRU Dijon.*

**Abstract**

*This paper presents the main differences existing in the elaboration process of law and standard and analyses their potential conflicts. It also describes the respective force of law and standards in three main areas : legal threat versus financial threat, conflict versus cooperation and finally their respective position faced to oligarchic power.*

*Keywords :*
law, standard, security, health information

## 1. Introduction

Perhaps because both the legislature and standards bodies produce official documents, they appear to have the same nature. These documents are written inside well representative institutions whose membership is not free but submitted to selective criteria and they are delivered after a long administrative process. However, this would be a fundamentally wrong interpretation of the situation. This short paper outlines how far the law and standards documents are from each other during their elaboration process and how close they are in the daily technical practice where the required standard can provide a perfect answer to a legal obligation. It describes and compares successively the elaboration process, their respective force and their mutual relations in a world where technical innovation, especially in the information technology field, goes faster than the public opinion which is the main determinant of the political power. Even the standards organizations have moved relatively fast in the field of healthcare informatics during the last two years but a brief outline of the situation is given in [1] and a more extensive description is available in this MEDSEC Handbook. The TC251 and ISO 215 standards activity can be accessed directly [2,3,4]. Further it may be expected that the International Electro-technical Commission standard 61508 parts 1 – 7 will provide a basis for the development of safe systems in Health Care in due course [5].
In the other hand, some industrials develops tools which quickly invades the market some times in few weeks and become a real life standard even if they are in clear opposition with the official standards. If institutions producing standard do not become able to provide pragmatic and easily readable standards corresponding to the industrial needs with delays compatible with the fast technical evolution, their utility could be seriously questioned.

## 2. Elaboration process of law and standards: democratic process versus aristocratic Process

In all democratic countries the law is the result of a process which guarantees that the legal text will represent the opinion of the majority of the citizens of the country. The most

common process is the elaboration of a bill by the Parliament or by the government, its discussion and its being voted into law by the Parliament. The members of Parliament are elected by all the citizens, most of the time through a direct vote, some times through an indirect vote by a "great elector" who has been previously elected through a direct vote.
The social profile of the Members of the Parliament reflects "globally" the social profile of the population of the country. By definition, Members of Parliament are not necessarily specialists either in the legal domain or in any kind of specific technological field. Thus, their decision to vote in favor or against proposed legislation is motivated by political considerations even if they try to be as informed as possible on the eventual technical consequences of their vote. The law may be considered at this point as a managerial decision; it provides a general orientation that defines the rules applicable to a general problem. The law will then be completed by other legal texts written most of the time by governmental officials involving both legal and technical specialists. However, even in the situation where the law is dealing with complex technical matters, the authors always try to describe the technical requirements in generic terms or by reference to existing standards.
On the other hand, the elaboration of standards appears more like an aristocratic or elitist process. The standards are proposed, discussed and voted inside the standards organization by members who are not elected by the general population but appointed by professional or commercial organizations at the national level or by the national standards organization for those who participate to the European Committee on Normalization (CEN) or to the International Standard Organization (ISO). The contents of a standard are purely technical. It reflects the rules of the professional, the state of the art, and also more and more often, the actual status of the market under the pressure of some "de facto" standard developed by a commercial organisation whose technology has achieved a dominant position. At the leading edge of technological development, there is a risk of embedding detailed technological material in a standard that is out of date before the standard has finished the validation circuit and its ratification by the standard organizations. This risk increases with the number of signatures required for the validation of the standard and this issue may become of major importance within the European Union. In order to reduce this risk, it is clear that, in fast moving technological fields, the standards must be oriented more as a kind of code of good practice, a set of guidelines on technical strategy than a list of detailed technical requirements. For example, it implies that the concept of using a smartcard to provide electronic signatures, for authentication, integrity protection, non-repudiation, can be considered as a mandatory requirement for having access to a medical network but that no length of the key shall be specified. Three years ago, a key length of 40 bytes was considered as providing a good level of security but this quite inadequate today.

### 3. The respective force of the law and standards: legal threat versus financial threats

The great force of the law lies in the fact that it is mandatory to respect it. Anyone infringing the law can be punished by severe penalties such as substantial fines or prison sentences. In many countries of Europe, an infringement of the law on "personal data protection" may lead to very significant penalties. For example, in France the use of personal medical data recorded in the hospital for another purpose than the care of the patients – without their informed consent – could lead to a maximum penalty of 30 000 Euros and 5 years of prison. This situation where the law punishes the unfair use of the personal data is very different from the situation, which exists in some other countries. The European directive on data protection, "On the protection of individuals with regard to the processing of personal data and on the free movement of such data", 95/46/EC, wad adopted on 24 October 1995. Among other things, the Directive describes the rules which have to be applied when people

want to exchange personal data with countries which do not provide adequate security guarantees.

The situation of the standards is quite different. By nature, they are strictly optional because the organization producing them has no opportunity to introduce any kind of constraint. Their force comes essentially from the market rules or from the market needs. A product that does not comply with relevant standards has less of a chance of competing successfully in the market place. The worse example, of course, is the electric plug which differs from country to country even inside Europe. No commercial organisation dares to propose an electric machine with a French plug in England and this just because nobody will be able to plug it without the use of an adaptator. In new technology, the problem is still the same. It would be highly risky to propose today computer communication systems which are not http compliant.

The force of a standard may also come from the product or service liability. In case of damages caused to a person, a judge may assess the liability of a supplier by examining if the product or the service has fulfilled the requirements of a skilled professional. Furthermore, the best definition of a skilled professional is one who follows the standards developed and accepted by his profession. Compliance to standards is not mandatory but ignoring them increases the risk of being considered as negligent – and consequently guilty – in case of litigation.

**4. Law and standards: conflict versus cooperation**

The possibility of a conflict between a standard and some legal requirements is unavoidable in the field of information technology where new concepts appear which have no equivalence in the legal domain. The law is always late because it reflects the political opinion and it is not surprising, therefore, that no clear legal solution is available to solve the different problems arising from the international development of the Internet. Some solutions will appear after the first litigation has occurred in case law using the legal concept of the present legislation even if it is not really adequate. The judge cannot say that there is no legal answer at a trial or after some new legislation has been enacted by the Parliament. It is, also, unavoidable that somebody could be found guilty for a fact which will become legal some months later although legislators try to avoid retrospective legislation. Before the new law it was a fault, a legal infringement, and the punishment can't be erased a posteriori; "Dura Lex sed Lex". The electronic signature in France has recently given illustration of conflict resolution between law and standards. France had a very restrictive position on cryptographic software and submitted to specific authorization which was not easy to get even for the use of such a security tool in medical data protection. The problem was that the development of electronic business requires the development of electronic signatures in order to secure the financial transactions and the "standard" was using cryptographic algorithms. So France was faced with the simple choice of changing its legislation to fulfill a de facto international standard or being excluded from the international electronic business.

On the other hand, standards may be also required by the law in order to avoid an uncontrolled development of technical solutions, incompatible with each other which could interfere with the objectives of the law. To continue the previous example, the law on electronic signature implicitly requires now the development of a standardized procedure for trans-border European recognition of Trusted Third Parties. At this point, standards may be considered as legal auxiliary. One example is the proposed standard which has been developed in the framework of the European committee for standardization, the working

group III 'security, safety and quality of healthcare information' of CEN TC251. According the European directive on data protection, European organizations cannot send personal data to countries, which do not present the same guarantees in their legislation as those required in Europe unless they make a contract in which the equivalent guarantees are defined. In order to help people define their needs clearly, a standard 'model contract guidance' which has been adopted by CEN [7].

## 5. Laws and standards faced to oligarchic power

Standard and law have in common the fact of elaborating their texts through a long discussion based mainly on a consensus research rather than a hard confrontation of experts sanctioned by a formal vote. This process may have two adverse effects: the standard may be out of date before being published or the "medium point" reached by the standard to get an agreement inside the group do not correspond to any kind of real industrial product. Even the decision process which goes from the proposal of a work item to its record of on the work plan could be too long to supply the market needs.
In the industrial area, the decision follows a quicker process. A product is designed to answer to a market study which has defined its characteristics and technician have to find technical solutions which must support the strategy decided by the management. When the product has been marketed in thousand samples it becomes a "de facto" standard to which the other industrials are obliged to comply. At this point, no other standards voted by any kind of standard board may affect the market rule. Even the law may not decide that some other standard should be used rather the one already used in the daily practice. It will be an offense to the market law and a kind of commercial protectionism which will not be accepted at the international level.
The only reaction may come from the juridical power if the "de facto" standard creates a "trust" which offenses some laws which exist in some countries.... Some example is well known of all of us. But whatever we may think about the "de facto" standards, their impact on the market is a clear demonstration of some failure of the administrative regulation of production. This situation rises some questions about the breach that exists between firms and standard organizations. Standard organizations often complain that industrials do not enough participate to their meeting or working group but do they propose a real fruitful ground for discussion, especially when the main part of the participant in the meeting are consultant selling their advises beside the working group or university people far away on economical consideration and more interested by some intellectually relevant problems than basic unavoidable technical requirements. In the security field, solutions will certainly come from law bodies and industry, forgetting to go through tiny door of the standard board. It's a pity but nightmare may become truth.

## 6. Conclusion

Law and standards even if they are the results of very different elaboration processes, are very complementary to each other. In a democracy, the power belongs to the Parliament and the last word will always stay in the hands of the national representatives. The aristocratic process which leads to an official standard or the oligarchic position of a dominant industrial which imposes a de facto standard are by nature submitted to the respect of the law but they may strongly – more and more in the future – influence the legislators in their decisions. The condition of this influence lies in its credibility proved by the ability to provide pragmatic and effective standards. The de facto standards, resulting from an oligarchic power, have a great advantage on this point and they present the danger that they can be widely accepted that they escape from any kind of political control. On the other hand, it implies that the

official standards organizations make a great effort to produce workable standards in good time, if they don't want to become only a kind of registration office for de facto standards. People who write the standards have to be conscious that the legislators have a great advantage which may be summarized in two Latin aphorisms, an old one and a new one: Dura Lex Sed Lex, even if the law appears unfair it is the law; "Mala Norma Non Est Norma", a bad standard will never be considered as a standard.

**7. References**

[1] B Barber, Patient data and security: an overview, Int J Med Inf, 49, 1998 19 – 30
[2] CEN Technical Committee 251 is accessed on www.centc251.org
[3] TC251 WGIII www.centc251.org as well as on the AFNOR site forum.afnor.fr
[4] International Standards Organisation ISO 215 www..iso.ch/meme/TC215
[5] International Electro-technical Commission standard 61508 parts 1 – 7, accessed on www.iec.ch
[6] Guide to Handling Personal Health Information in International Applications in the Context of the EU data Protection Directive, version 1.4, June 2000, CEN TC251 WGIII, Brussels, and British Standards Institution, IST/35, London

**8. Address for correspondence**

Professeur François André ALLAERT
Service de Biostatistique et Informatique Médicale
Centre Hospitalier Universitaire de Dijon
BP 77908
21079 DIJON CEDEX
Tel : 33 3 80 29 34 31
Fax : 33 3 80 29 39 73
Email: allaret@ipac.fr