



eHealth in Belgium, a new “secure” federal network: Role of patients, health professions and social security services

Francis Roger France*

School of Public Health, Health Services Research, Université Catholique de Louvain, Brussels, Belgium

ARTICLE INFO

Article history:

Received 8 September 2010

Accepted 2 October 2010

Keywords:

Health networks

Security risks

Encryption

Patient empowerment

ABSTRACT

eHealth platform is the official federal network in Belgium (created by law on 21 August 2008) devoted to a secure exchange of health data in many types of applications, such as health care purposes, simplification of administrative procedures and contribution to health policy. It implies a controlled access to decentralized databases and uses encrypted personal data. The national identification number has been chosen in order to authenticate the requester, the patient, and the receiver of information exchange. Authorizations have to be respected in order to obtain personal health data.

Several questions are raised about its security: the lack of mandatory request for systematic journaling on accesses to the electronic patient record as well as the absence of explicit procedures for sanctions in case of unauthorized access, the new role of social security administration in managing security where a eHealth manager can be both judge and party (in the function of trusted third party for health data encryption and of a required lawyer for texts proposed by physicians to the Commission for the protection of private life). Another critic concerns the number of physicians in minority and the absence of patients' delegates in the eHealth Board. At a time when the patient is becoming a partner in the care team, should not he be the gate-keeper for the access to his own health record? How could networks help him to get the appropriate knowledge to contribute to care and to write his testament of life? Recent laws (on private life, patient rights and euthanasia) have contributed to a behavioural change in citizens and physician attitudes.

Recommendations are made in order to improve the acceptability of eHealth platform.

© 2010 Elsevier Ireland Ltd. All rights reserved.

1. Introduction: impact of cultural and social factors on health care systems

Even in an era of globalisation, cultural and social factors remain strong determinants of health care systems [1]. Belgium is a small country (1/18 of France), with a high density of inhabitants (10.2 million), three regions (Flanders, Wallony and Brussels) and three Communities (speaking Dutch, French

and German). All Belgian citizens are now covered by the social security system. It is based on an agreement obtained inside INAMI (National Institute against Illness and Disability) between representatives of physicians unions and delegates of “mutualities” (mutual-benefit societies). The amounts of fee for services are adapted by them in a nomenclature of procedures and drugs. In complement, a lump sum is fixed for each hospital day of stay by the Federal Public Health Service, while taking in account Diagnosis Related Groups.

* Tel.: +32 23753748.

E-mail address: frf@skynet.be.

1386-5056/\$ – see front matter © 2010 Elsevier Ireland Ltd. All rights reserved.

doi:[10.1016/j.ijmedinf.2010.10.005](https://doi.org/10.1016/j.ijmedinf.2010.10.005)

2. The eHealth platform: a public institution in social security

The federal health network, called *eHealth platform*, has been created by a law on 21 August 2008 [2]. It is “a public institution in social security” acting for missions through contracts with the Federal State, similarly to the *Crossroads Bank for Social Security* (CRBSS) that is functional since 1990 [3]. It benefits from the work done since 1999 by the Federal Commission “Norms for Telematics in Health Care” [4,5] for health information exchange through networks: XML format in KMEHR, coding in ICD-9-CM and 10, using ICF and LOINC, as well as DICOM for images.

2.1. Objectives and missions

eHealth has three main objectives: (1) to optimize quality and continuity of health care as well as patient safety; (2) to simplify administrative tasks; and (3) to contribute to public health policy. These objectives have to be reached by services production and by exchanges of electronic information between all health care actors, while assuring data security and private life protection. Several missions are attributed to the eHealth institution in order to accomplish these objectives, among which to develop a vision and a strategy; to establish norms, standards and ICT specifications, as well as a service oriented architecture; to check if software of electronic patients records utilizes these norms.

eHealth management has to conceive and develop basic services, free of charge, that can help all health care actors.

2.2. Security technical aspects

The unique identification number distributed by all communes to all citizens and foreign workers between 2007 and 2009 is available on chip cards (identity and social security cards). This “national number”, authenticated by the communal administration, has been chosen for health information exchange, in order to authenticate the requester, the patient and the receiver. eHealth provides the software that allows to read the chip card content through a specific reader. The same software is currently used widely in Belgium, for many electronic exchanges: tax return, birth declaration, retirement estimates, as well as eHealth applications that will be described hereafter (Section 2.3). The Parliament accepted the “national number” not to be replaced by a specific “health care number”, as too many persons could have to know this substitute number and as cost and risk of error were high. It was accepted to encrypt the “national number” as well as the message content to assure confidentiality.

Institutions can have access to eHealth through a “certificate” made of 2 keys to be authenticated and a specific Web access signature.

Among **Basic Services of the platform** (at the center of Fig. 1), offered to users, there are:

- **Integrated management of users and authorized accesses:** authorizations are kept in a register, as only authorized users can have access to personal health data. Each iden-

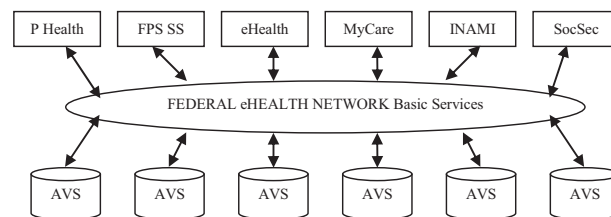


Fig. 1 – eHealth platform.

tified and authenticated requester asks access through a “policy enforcement point” (PEP), that checks user’s identification, reason for access, context, conditions for access. Decision is made through a “policy decision point” (PDP) in relation to the content of the authorization register and of policy information rules. A user (physician or institution) can have an authorized proxy, like a secretary, mandated for a period of time.

- **Loggings:** a security system registers all requests (users identification, time stamping, motive of access).
- **End-to-end encryption and anonymization:** for a secure exchange of personal health data, a public key (in a library) and a private key (only known by the user, with an authenticated certificate) are provided by eHealth, that acts as connecting body (end-to-end asymmetric encryption). The system provides a software that generates locally asymmetric keys. The private key has to be securely kept by the user who generated the two keys, while the public key is sent to a library.

The national number of the patient as well as the message content is crypted.

Some messages are not addressed, when the receiver is unknown, like a pharmacist when a drug is prescribed. In this application, the message (prescription) is crypted with a symmetric key sent to him by a center of deposit of keys. The encrypted message is sent independently to a deposit of crypted messages. The pharmacist will have to justify the right to obtain access to the key deposit as well as to the message deposit, using his symmetric public key. Only the author of the message (prescriber) and the deposit of messages can decrypt, with the private key, the asymmetric part of the crypted message. The deposit of keys and the deposit of messages are separate entities.

- **Portals:** each portal is an entry point to Internet, in order to access on line to health information. eHealth provides a content management system as well as a research motor, using keywords.

2.3. Management and organization

The “management committee” of eHealth is made of members appointed by “mutualities”, public services, and health professions. A “concertation committee” has been appointed, with representatives from regional health networks initiatives, and several experts.

A “Social Security and Health Sector Committee (SS&HCttee)” has been created inside the Commission for the protection of private life. Its two sections (SS&H) have to formulate recommendations (to be checked by a

lawyer, the general manager of eHealth) about security for personal health data transfer and processing. They have to be consulted in order to give access authorization in any case not specified by the law. They receive all complaints in case of infraction to security for electronic personal health data.

In order to assure security, eHealth Management Committee nominates among members of its personnel: (1) an advisor in information security and (2) a physician in charge of surveillance of personal health data processing. These two “information officers” receive specific instructions from the SS&HCttee.

2.4. Working applications

Fig. 1 shows how eHealth works in practice (see <https://www.ehealth.fgov.be>).

The eHealth platform allows exchange of data between users through portals represented by boxes in the upper part of the figure.

Patients, health professionals, hospital managers and mutual-benefit societies as well as other insurers have access, when authorized, to eHealth national applications through AVA (Added Value Applications), such as electronic drug prescription, birth declaration, H1N1 epidemic monitoring, orthopaedic prosthesis register, cancer register, testament of life, willingness or not to give an organ, wish for euthanasia, electronic transfer of bills to mutualities, etc.

These portals are currently working in a diversified institutional environment:

- The Federal Public Service (FPS) of Public Health processes statistical data, DRG data, clinical pathways, disease registers, etc.
- The FPS for Social Security has a portal devoted to citizens questions, to knowledge bases or about their electronic health record.
- Mycarenet is a patient data exchange system for electronic administrative and financial data, between health care institutions and mutualities,
- The INAMI portal is devoted mainly to Federal annual expenses, budget estimates and validation tests, etc.

Basic Services of the Platform (BSP) (described in Section 2.2) are offered on the central ICT infrastructure of eHealth (at the centre of Figure 1) (authorized accesses, loggings, portals, letter box for each health provider, end to end encryption and anonymization, references to authorization link between patient and physicians). Before each application, flexibility studies are made (meetings between eHealth managers and groups of users, definition of access rules, specific developments, tests, etc.).

Authentic Validated Sources (AVS) are described, in the lower part of Fig. 1: several databanks are linked to eHealth. Information can be accessed by authorized users to get the best validated source of information. For examples:

- The national register contains information transferred by communes (citizen identification: name, first name, sex, date, place of birth, national number).

- The INAMI generates physician identification numbers and manages all patients bills sent by various mutualities.
- The FPS of Public Health processes the content of patient minimum basic data sets sent by all hospitals, etc.
- Knowledge bases about drugs, diseases can also be accessed.

These AVS are under the responsibility of their own manager, who has to assure the quality of the information provided. This lower part of Fig. 1 is the domain of Service Providers or Health Information Suppliers. Among the publicly available applications through eHealth platform, let's quote: registers of health professionals: physicians, pharmacists, nurses; INAMI agreement for reimbursement, etc.

3. Reassuring and worrying security features of the eHealth platform

The eHealth platform is perceived as a step forward for health data exchange and processing in Belgium. However, physicians have been frustrated not to be associated closely since the beginning to the development of the project. It was initiated by the administrator of the Crossroads Bank for Social Security, with a strong support from “Mutualities” and INAMI, and put in the hands of social security personnel, with a minority of physicians in the Management Committee, and no representative from patients associations, despite their request. When it was installed, a leader of the largest union of physicians agreed to be appointed as chairman of the management committee, but one of his colleagues introduced an appeal against the law creating eHealth.

3.1. At a first glance, there are reassuring features:

- It is claimed that no central database of personal health data exists in eHealth.
- The platform is only a network to exchange secured personal health data between all actors in the health care sector.
- With patient consent, references to location of his health information are made available (no access to this data base content without specific authorization).
- The law on eHealth applies what is required by the laws on protection of private life, professional secrecy, patient rights and on the practice of medicine.
- Access is strictly controlled: what actors, for what data type, about which patients, for what period of time.
- Each requester and each patient is identified and authenticated by the national citizen number, with qualification and role specified for the requester (for example, a general practitioner, acting as a consultant or for an insurance).
- All personal health data to be exchanged are crypted.
- The use of eHealth platform is optional, not mandatory.
- Security aspects and authorizations are under the control of the Sectoral Committee Health and Social Security of the Commission for the protection of private life.
- An evaluation of security leaks will be done by the Parliament two years after the publication of the law (in August 2010).

3.2. However, an analysis of what is done in practice is worrying

- Our main concern is the absence of mandatory journaling in order to monitor accesses to the electronic patient record. At a time when the “paper less” record becomes a reality, the most elementary security measure [6] appears to require on the first screen of any accessed record the inerasable list of all persons who obtained access, with time stamping. Such a list should also be made available by citizen for all accesses to health personal data through eHealth. Each patient should be able to check who had access to his record. It would best prevent illegitimate curiosity.
- Another point is the lack of explicit procedures for sanctions in case of unauthorized access to sensible identified health data. Outside of Courts of Justice, sanctions are rarely applied.
- When physician unions learned that the general manager of the eHealth platform is also general manager of the Crossroads Bank for Social Security, CEO of the SMALS that encrypts data, strategic advisor in FEDICT that supervises SMALS and member of the Belgian Commission for the protection of private life, they felt unacceptable to have the same man, as honest as he can claim, to be simultaneously judge and party.
- Representatives of patients were refused to be nominated in the eHealth platform management. Checking identity falsifications, illegitimate accesses and illegal gains should be planned in order to obtain their confidence.

4. Legal “beaconing” of the patient, as gatekeeper for eHealth accesses

We strongly believe that the patient is the best gatekeeper for the access to his own personal health data. It has been recommended by IMIA Working Group on security in health information systems at the Dijon conference in 2006 [7]. Several laws have been adopted in Belgium that regulate the circumstances in which the patient can experiment his autonomy, give him access to his electronic health record, and protect his private life. They had a great influence not only on the development of citizen empowerment in health care, but also on a change in behaviour of physicians and other health professionals. The following laws accomplished this change in society:

- The law of 08 December 1992 on protection of private life in relation to personal data processing, with the Commission and the sectoral Committee [8].
- The law of 22 August 2002 on patient rights, among which information about his disease and his treatment and access to a copy of his medical record [9].
- The law of 28 May 2002 on euthanasia, which is not a patient right, but a way not to condemn the physician who accomplished it, if explicit conditions were respected [10].

5. Recommendations

In practice, we believe that the eHealth platform would be better accepted if the following measures were applied:

1. To provide a systematic and complete list monitoring all accesses to personal health data through the eHealth platform, by citizen. Such list should be consulted directly by the concerned patient and by persons explicitly mandated by the Health section of the sectoral Committee of the Commission for the protection of private life, as well as health personnel designated by the patient.
2. To establish a list of sanctions for unauthorized accesses, fraud in identification and damages caused to the patient by confidential information leakage as well as procedures for obtaining appropriate documentation and investigation. Instances mandated to apply these sanctions independently have to be identified and their actions evaluated.
3. To test systematically the level of security of the eHealth platform by reviewing with patients the list of accesses to their record (patients selected randomly and cases with expected high incidence of unauthorized accesses such as public personalities). Publish yearly results and follow up (sanctions taken or not).
4. To entrust an independent organization (with no authoritative link with eHealth management) for health personal data encryption (a trusted third party).
5. To control every access to all databases that could be managed by eHealth associated personnel (like a data repository on authorizations of access to patients personal data), as well as to any other data base, even anonymous (that might generate illegitimate gain like prescription profiles).
6. To check systematically every request for return to identification of a citizen in any data base containing anonymous health data (like genetic registers).
7. To explore systematically eventual data linkage by citizen between eHealth platform and the Crossroads Bank for Social Security (for example linkage of penal records with tax payment and drugs prescribed). To verify if the use of the national number has been appropriate and check for eventual abuses (social security number falsification, as documented in France and in the USA).
8. To nominate patients representatives in the eHealth Board and to specify with them how and by whom, for what purpose their personal data can be used.
9. To establish a procedure by which physicians have to be consulted to express their voice for health matters; to revise representativity of physicians in eHealth Board, and to appoint an independent lawyer as censor for physicians text proposals in the Commission for protection of private life.
10. To detect systematically fraud in health data banks access, mainly for financial profit.

Summary points

- Very few countries have a functional national identification number, as in Belgium, that can be used in order to obtain access to personal patient data.
- The choice of this number raises questions about security of patient rights.
- Although several original methods have been applied in a new national health network, in order to protect security of access to authorized persons, there are unfortunately still important missing features or procedures that are identified in this paper.
- Ten recommendations are made in order to improve the acceptability of this eHealth platform.
- They have a universal character as they were adopted in the recommendations of the Hiroshima IMIA conference on Security in Health Care in November 2009.

REFERENCES

- [1] J.R. Kimberly, G. de Pouvourville, T. D'Aunno, *The Globalization of Managerial Innovation in Health Care*, Cambridge University Press, United Kingdom, 2008, 379 pp.
- [2] Loi du 21.08.2008 relative à l'institution et à l'organisation de la plateforme eHealth (Law installing and organizing eHealth platform in Belgium), Moniteur Belge, 13.10.2008.

- [3] Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une banque-carrefour de la sécurité sociale (Law installing and organising a crossroads bank for social security), Moniteur Belge, 22.02.1990.
- [4] Arrêté Royal du 3 mai 1999. Commission Normes en matière de Télématique dans le secteur des soins de santé (Royal Decree: Commission Norms for Telematics in H.C.).
- [5] F.H. Roger France, M. Bangels, *Norms for Telematics in Health Care: priorities in Belgium*, vol. 93, IOS Press, 2002, pp. 179–183.
- [6] Ishtar Consortium, *Implementing Secure Healthcare Telematics in Europe*, vol. 61, IOS Press, The Netherlands, 2001, 351 pp.
- [7] J.R. Moehr, F. Allaert, E.H. Kluge, C. Quantin, F.H. Roger France, *Secure eHealth: managing risk to patient data, Recommendations of IMIA WG*, *Int. J. Med. Inform.* 76 (2007) 398–399.
- [8] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (Law to protect private life in relation to personal data processing), Moniteur Belge 18.03.1993.
- [9] Loi du 22.08.2002 relative aux droits des patients (Law on patients rights), Moniteur Belge, 26.09.2002.
- [10] Loi du 28.05.2002 relative à l'euthanasie (Law on euthanasia), Moniteur Belge, 22.06.2002.

FURTHER READING

- [11] <https://www.ehealth.fgov.be> – Federal platform eHealth.
- [12] <http://www.reseausantewallon.be> – Health network in Wallony.
- [13] <http://www.gzi.be> – Gents Ziekenhuis Overleg.