The law on electronic medical prescriptions

FRANCIS DE CLIPPELE

Introduction

The adoption of electronic medical prescriptions is part of a wider European health policy[1] that aims at rationalizing healthcare and the use of medication[2] by implementing information and communications technologies applications (ICT) and promoting generic medication,[3] Although, according to article 152 of the EC Treaty, and particularly in its paragraph 5, Community action in the field of public health must fully respect the competence of the Member States.

It is expected that the application of ICT can improve access to healthcare and boost the quality and effectiveness of the services offered.[4] It is an ambition of the European Union to build a framework on a wide range of European policies and best practices, a 'European e-Health Area'. E-Health plays a clear role in the European Union's eEurope strategy to achieving stronger growth and creating highly qualified jobs in a dynamic, knowledge based economy[5] – the vision set out by the Lisbon European Council in March 2000.[6] The European policy on e-health is also intended to offer an answer to the increasing mobility of patients[7] and health professionals within an internal market.[8] It is believed that e-Healthcare is one aspect of the answer to face major challenges: guaranteeing accessibility, quality and financial viability of a health care service for everyone in an ageing society.[9]

The electronic medical prescription is key to achieving the European e-Health policy. The legal acceptance of electronic documents in a secure environment is a prerequisite for electronic medical prescriptions. The requirement for confidentiality and consumer confidence makes health information systems security critical. Furthermore the implementation of new technology must not infringe on patients' rights.

[1] Community Public Health Program referred to in Decision 1786/2002/EC of the European Parliament and of the Council of 23 September 2002 adopting a program of Community action of public Health (2003-2008), OJL 271 of 9 October 2002.

[2] One of the minor expectations is also that the e-prescriptions will reduce the risk of medication errors due to illegible handwriting.

[3] There is a growing list of European countries that are currently in different stages of modernizing their medical prescription practices. In Sweden, where e-prescriptions were introduced as early as 2000 in some regions, over four prescriptions out of ten in Stockholm are now electronic. About 16.000 prescriptions are now sent electronically to the city's pharmacies every week, and a majority of prescriptions are expected to be electronic at the end of this year. In Finland several e-prescription pilots were launched in 2003-2004 and similar initiatives are currently being studied in France, Portugal and Germany. Germany is planning to introduce electronic medical prescriptions in 2006 after the launch of its e-health insurance card.

[4] 'e-Health-making healthcare better for European citizens: An action plan for a European e-Health Area', *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee of the regions.*

[5] e-Health-making healthcare better for European citizens: An action plan for a European e-Health Area', *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee of the regions.* COM (2004) 356 Final 30 April 2004 available in electronic format at http://europa.eu.int/comm/health/ph_information/e_health/e_health_en.htm.

[6] European Council (2000), *Presidency Conclusions.* Lisbon European Council. 23-24 March, 2000 COM (2002) 263 final 05.12.2001. *eEurope 2005: An information society for all: An action plan to be presented in view of the Sevilla European Council, 21/22 June 2002*, Brussels, 28.5.2000. Available in electronic format at http://www.europarl.eu.int/summits/lis1_en.htm.

[7] Patient mobility is addressed specifically in a Communication from the Commission, COM (2004), 301.

[8] Regulation 1408/71 that co-ordinates social security legal schemes has recently been amended to streamline and modernize access to health care across borders, particularly when undue delays occur in the patient's home Member state. In January 2004 the Commission adopted a proposal for a Directive on services in the internal market, including health services and for the reimbursement of by the relevant health insurance institutions when healthcare is provided in another Member State.

[9] See also COM (2001) 723 final 05.12.2001.

A signature is the expression of approval of the author with the content of a writing to which he consents and accepts the legal consequences

The legal acceptance of electronic documents

The employment of electronic documents implies the legal acceptance of digital data that cannot contain a manuscript signature. Every digital copy is an original, and every copy can be modified without its changes being visible. The authenticity and integrity of the electronic documents are therefore of legal concern.[10]

A signature is the expression of approval of the author with the content of a writing to which he consents and accepts the legal consequences.[11] In order to attach legal effect to a signature, one has to ascertain its origin. The signature is unique. Indeed the identification of the signature guarantees the non-repudiation of the will of the person behind the signature. The author of the signature must be the one who is committed. The need to identify a person unambiguously is a most important component of the interoperability of health information systems. The eEurope2005 action plan already supports the development of standards for a common approach to patient identifiers and electronic health record architecture.

The electronic signature

The development of the electronic transfer of documents requires the legal acceptance of electronic signatures.[12] The acceptance of electronic signatures is subject to recent legislation: (1) The law of October 20, 2000 introducing the legal use of information technology and electronic signatures into judicial and extra-judicial procedures, and (2) the law of July 9, 2001 inserting the legal rules on electronic signatures and certification authorities.[13]

The legislator has chosen not to define the electronic signature. Nevertheless an electronic signature shall have legal effect when two conditions have been satisfied, namely the assignment to a natural person and the guarantee of integrity of the private deed. The objective of the legislator was to secure the transfer of electronic data. The insecurity of the virtual assignment of documents is the effect of dematerialization of data and its storage medium.[14] The insecurity is also related to the possibility of easy copying[15] and invisible or untraceable[16] and even non-repairable interferences.[17] The electronic transfer of data is also characterized by increasing anonymity[18] and the need to protect the privacy.

The legal protection of the privacy and consumer rights

The confidentiality and protection of patient data is governed by the general European Union rules of data protection, as well as by the requirements of ePrivacy legislation regarding communications infrastructure.[19] The requirement for confidentiality calls for high quality security systems. The electronic commerce Directive[20] also applies to the provision of on-line health services. The Directive contributes to the legal certainty and clarity needed for the provision of on-line information services, with information and transparency requirements and the liability of intermediary service providers, thus increasing consumer confidence. The personal life may only be safeguarded by the legal warrant of

[10] Cfr. R. DE CORTE, "Elektronische handtekening en identificatie in de virtuele wereld", *P&B* 2001, 212.
[11] M. VAN QUICKENBORNE, "Quelques réflexions sur la signature des actes sous seing privé", *R.C.J.B.* 1985, p.57; H. DE PAGE, *Traité élémentaire de droit civil belge,* III, Brussel, Bruylant, 1967, p. 756, nr. 774.
[12] D. SYX, "Vers de nouvelles formes de signature? Le problème de la signature dans les rapports juridiques électroniques», *Dr. Inform.* 1986/3, p. 133; E. DAVIO, «Preuves et certification sur internet», *T.B.H.* 1997, p. 660; D. GOBERT en E. MONTERRO, «L'ouverture de la preuve littérale aux écrits sous forme électronique», *J.T.* 2001, p. 114.
[13] Wet 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en buitengerechtelijke procedure, *B.S.* 22 december 2000; Wet 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridische kader voor elektronische handtekeningen en certificatiediensten, *B.S.* 29 september 2001 (www.staatsblad.be), implementing the EU Directive 99/93/EC OJL 13, 19.
[14] B. DE GROOTE, "Het bewijs in de elektronische handel – enkele bedenkingen", *A.J.T.* 2000-2001, nr. 22; R. DE CORTE, "Elektronische handtekening en identificatie in de virtuele wereld", *P & B* 2001, 208.
[15] We think of the possible consequences of a computer virus.
[16] Unauthorized alteration of electronic data can be difficult to detect.
[17] ICT criminality has no borders. The place of the offence is not necessarily the place where the effects are shown. See also R. DE CORTE, "Elektronische handtekening en identificatie in de virtuele wereld", *P & B* 2001, 209.
[18] The expedition of e-mails on a 'fictitious' address or the use of a nickname in a chatbox is common practice. See also G. BALLON, "Ik gaf mijzelf (g)een naam, over anoniem en pseudoniem optreden in de openbaarheid", *T.P.R.* 1981, 557-592; R. DE CORTE, "Elektronische handtekening en identificatie in de virtuele wereld", *P & B* 2001, 211 e.v.
[19] See for example, the *Data Protection Directive* 95/46/EC OJL 281, 23 November 1995 and the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12), or the *Telecommunications Privacy Directive* 02/58/EC OJL 281, 31 July 2002, replacing EC Directive 97/66/EC.
[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJL 178, 17 July 2000, p. 1.

confidentiality of the electronic data. Confidentiality implies the protection of electronic data against entry or knowledge by any unauthorized third party. The confidentiality of an electronic notice is secured by encryption.

Asymmetrical encryption implies a double security with a private key (known only by its owner) and a public key (made available through a certification authority at disposal of a third party).[21] Both keys are complementary through an algorithm function, which creates the digital reproduction of the notice. The sender of the electronic notice (the certification holder) signs the notice with his private key and conveys the access code (public key) to a third party by intervention of the certification authority The electronic signature based on asymmetric encryption (i.e. a digital signature) has an equivalent legal value as the handwritten signature.

The electronic signature based on cryptography[22] complies with the legal necessity of identification and assignment. These two conditions are also applicable to handwritten signatures.[23] The digital signature is therefore a sealed combination of figures and letters sent in attachment to an electronic notice and which can only be opened by means of the public key. The public key is secured by the certificate sent with the message and ascertained or authenticated from a certification authority recognized as such by the Minister of Economic Affairs. The legal acceptance of the electronic signature is based on the European Directive.[24]

The certificate is defined under article 2, 3 of the Law of July 9, 2001 as *'an electronic confirmation of the data of the signature and the identification tool of the natural or corporate person committed'*.[25] The certificate is an electronic file for authentication sent together with the electronically signed notice. The qualified certificate is an electronic file that fulfills the legal requirements and that is issued by an authorized certifier.

The electronic signature is therefore a necessary tool for the electronic medical prescription. By means of an electronic qualified signature, the medical doctor may electronically send a secure and certified medical prescription (indirectly) to the pharmacist. By means of the electronic signature the patient may also correspond individually and safely with the on-line pharmacist.

Electronic reporting, storage and transfer of medical data

Following article 9bis of the Law of July 14, 1994 on the insurance for medical treatment and allowances (*M.O.* 27 August 1994, hereafter GVU),[26] as modified by article 75 of the Law of February 22, 1998, medical data may be stored electronically and shared by healthcare services. The electronic reporting and communication of data is not further defined. The law has adopted a technological neutral stance. The law covers photographical, optical, electronic, magnetic or any other technique. Healthcare services that offer medical interventions covered by the social security allowance shall provide the patient (article 32 GVA) with a certificate of the intervention (Article 34 GVU) and a prescription for medication (Article 53 GVU). The certificate or the prescription shall bear the signature of the health care service. The prescription will moreover contain a unique sequence number and identification number of the prescriber (Article 73bis GVU, Royal Decree April 11, 1999).[27]

A model for electronic medical prescriptions

The electronic medical prescription is legally only acceptable when it is technically secured and technology-neutral to be useable for independent medical doctors and pharmacists. A model has been proposed based on standard protocols (TCP/IP, Internet), which can be used independently of the computer platform. The electronic medical prescription shall be linked to the electronic medical report of the general practitioner.

[21] Cfr. V. VANDENABEELE, "De elektronische handtekening : rechten en plichten van de certificatiedienstverlener, de certificatiehouder en de vertrouwende derde", *T.B.B.R.* 2002, 610.
[22] J. DUMORTIER en P. VAN EECKE, "Naar een juridische regeling van de digitale handtekening in België", *Computerrecht* 1997, 4, 154.
[23] Cass. 28 juni 1982, *R.C.J.B.* 1985, 57, noot VAN QUICKENBORNE, M.
[24] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 19.1.2000 L13/12).
[25] V. VAN DENABEELE, "De elektronische handtekening: rechten en plichten van de certificatiedienstverlener, de certificatiehouder en de vertrouwende derde", *T.B.B.R.* 2002, 611. With data for the creation of a signature is meant in the Law of 9 July 2001 the private key, with the data to verify the signature in meant the public key.
[26] Wet van 14 juli 1994 betreffende de verplichte verzekering voor geneeskundige verzorging en uitkeringen, *B.S.* 27 augustus 1994, zoals gewijzigd bij artikel 75 van de Wet van 22 februari 1998 (www.staatsblad.be).
[27] K.B. 11 april 1999 tot wijziging van het Koninklijk Besluit van 8 juni 1994 tot vaststelling van het model van voorschrijfdocument betreffende de verstrekkingen van farmaceutische producten ten behoeve van niet in een ziekenhuis opgenomen rechthebbenden, *B.S.* 23 april 1999 (www.staatsblad.be).

One should carefully watch the privacy when deploying a system through a central server

A system by which the electronic medical prescription is sent directly to the pharmacist is legally not acceptable. A direct communication with the pharmacist would infringe the freedom of the patient to choose his pharmacist. The medical doctor therefore will send the electronic medical prescription to a central server from which the pharmacist chosen by the patient may collect the prescription. One should carefully watch the privacy when deploying a system through a central server. Such a system may legally only be enforced when the medical doctor,[28] the pharmacist[29] and the patient[30] have a unique, non-transferable identity code which is sufficiently secured. The model for the electronic medical prescription shall be adapted to the Belgian social security system deploying a central server(s) in combination with log files that are linked to the SIS-card[31] and the electronic medical report.[32] The electronic medical prescription will also contain an ID-number created by the software of the medical doctor and securely sent to the server. The ID-number can be the RIZIV-number of the medical doctor added with date of issuance. In this manner, with an ID-number of the medical doctor, an ID-number of the pharmacist, an ID-number of the patient and an ID-number of the prescription, the system is able to identify the individual and controllable, so that the security of the electronic communication and the administration thereof, the system of the electronic medical prescription is legally reliable and acceptable.

In order to avoid any abuse, one prescription should contain one medication only. The relation between electronic medical prescriptions is, however, recommended for a medical doctor to indicate the combination of medications prescribed. All pharmaceutical products will be sent through a coding system (CNK). The magisterial preparations will be inserted in a (free) format on the electronic medical prescription.

An electronic medical prescription should be considered as a particular form of communication or exchange between health care services. The communication is performed on-line within a closed circuit with every prescription containing one medication, and in an attachment after encrypting the ID numbers of the health care services and the patient sent to a central server. The electronic medical prescription will be necessary for the on-line sale of pharmaceutical products subject to prescription.

An electronic medical prescription is therefore a non-addressed notice because at the moment of sending the consignee, the pharmacist, is still unknown. The patient is entitled to a free choice of his pharmacist. The power of decision of the patient is not only related to the choice of the pharmacist but also 'to or not to' contact a pharmacist for the presentation of the prescription.

For this purpose, the electronic medical prescription is sent to a third administrator. It is preferable that the (central) server, intervening as trusted third party, automatically sends a (solely technical) receipt message to the sender. One can also think at the option of the patient of a receipt message from the consignee, a pharmacist. The latter receipt message is distinct from the solely technical receipt message because it also informs on the outcome or use of the prescription.

The automatic technical receipt message may be used as the start of the limited life of the electronic medical prescription. It is preferable that after a certain period, defined by law, the electronic prescription will be invalid. The patient should be informed of the invalidity. The patient then should have the choice whether the sender, medical doctor, shall be informed of the fact that the prescription was not used and therefore annulled.

Conclusion

E-health, the application of information and communications technologies (ICT) that affect the health care sector, is developing fast in Europe. In this respect, the European Commission's e-Health Action plan, adopted on 30 April 2004, covers a wide range of issues and applications from electronic prescriptions and computerized health records. A model of the electronic medical prescription must respect patients' rights and can only be deployed in a system of security in order to protect the confidentiality. ■

Francis de Clippele is a lawyer at the Antwerp bar in Belgium, practicing in general commercial, trade and company law matters. His practice is now focused on new technology and computer law. Francis is also a lecturer at the University of Antwerp.
His academic activities are reflected in numerous publications on ICT-law, corporate governance and transport law.

http://www.declippeleadvocaten.com
francis@declippeleadvocaten.com

[28] We had thought of the social security number of the medical doctor (RIZIV-number).
[29] We had thought of the APB-number of the pharmacist.
[30] We had thought of the SIS number for the patient. A patient's identifier included in the European Health Insurance Card (OJEU 27 October 2003) includes the patient's personal identification number as part of the data allowing people to use the card to get treatment outside their home Member State. By the end of 2006, Member States, in collaboration with the European Commission, should identify a common approach to patient identifiers. This should take account of best practices and developments.
[31] K.B. 22 februari 1998 houdende uitvoeringsmaatregelen inzake de sociale identiteitskaart, *B.S.* 13 maart 1998 (www.staatsblad.be). The health care services must, in order to fulfill their obligations under the third-payer system, use the social identity card (SIS) of the insured.
[32] It is the electronic administration of a global medical file of the patient.