

# Support for Electronic Health Records in Czech Law

Otto Dostál<sup>1</sup>, Milan Šárek<sup>2</sup>

<sup>1</sup> Masaryk University, Institute of Computer Science, Brno, Czech Republic

<sup>2</sup> Institute of Computer Science AS CR, Department of Medical Informatics, Prague, Czech Republic

## Abstract

The spreading use of the e-Health applications in healthcare raises questions about the legal aspects of this development. In this paper, we wanted to look into such questions related to one of the most basic elements of any e-Health solution - electronic health records - in Czech law. The article aimed to create a review of the national legislation related to electronic health records currently in force (which means primarily the Care for Health of the People Act n. 20/1966 Sb.), and to identify possible legal issues that could be preventing the deployment of e-Health Applications.

The article shows that the Czech law indeed allows usage of electronic health records, and sets relatively detailed rules in some areas such as what information must be included inside it, and how to archive the data. However, it offers little guidance regarding some other situations, like it is ignoring the question of technical standards for interoperability. The briefness of the Act leaves lot of the decisions related to the development of the e-Health applications up to the individual healthcare facilities.

## Keywords

e-Health, electronic health record, legal framework, Care for Health of the People Act, advanced electronic signature

## Correspondence to:

### Otto Dostál

Masaryk University, Institute of Computer Science  
Address: Botanická 554/68a, Ponava, Brno, Czech Republic  
E-mail: ottodostal@gmail.com

EJBI 2012; 8(2):29–33

received: June 21, 2011

accepted: January 16, 2012

published: June 15, 2012

## 1 Introduction

The incorporation of various information technology tools in medical practice brings opportunities related to improvement of quality and availability of services and other benefits. However, the spreading use of the e-Health applications in healthcare also raises questions about the legal aspects of this development. In this paper, we would like to look into such questions related to one of the most basic elements of any e-Health solution - electronic health records - in Czech law.

The legal framework for the management of electronic health records forms the basis both for the successful design of electronic health records, and for the subsequent management of the whole process of documentation. The process of documentation starts from the creation of the data in medical facilities and continues with its storage and subsequent archiving, but includes also the transfer of medical data extramural outside the hospital information system. This article aims to create a review of the national legislation related to electronic health records currently in force, and to identify possible legal issues that could be preventing the deployment of e-Health Applications. The article would also like to possibly arouse discussion on this crucial issue. Discussion could contribute to the further

development of e-Health applications, which could then facilitate the implementation of EU priorities promoting the mobility of EU citizens as described for example in the report of the EU on e-Health infrastructures from January 2011 [1].

## 2 Relevant Statutes

The legal framework in the Czech Republic related to the problematic of electronic health records consists of several acts [2], primarily the n. 20/1966 Sb. Care for Health of the People Act, the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Signature Act.

In this article, we will concentrate mostly on the n. 20/1966 Sb. Care for Health of the People Act (hereinafter referred only as “Care for Health of the People Act” or “Act”). The reason for this is, that the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Signature Act are more general types of statutes, while Care for Health of the People Act incorporates the core of the legal regulation of health records, including the electronic variant. Also, the n. 101/2000 Sb. Personal Data Protection Act and the n. 227/2000 Sb. Digital Sig-

nature Act are heavily influenced by the European Union legislation they are implementing (Directive n. 95/46/ES on the protection of individuals with regard to the processing of personal data and on the free movement of such data [3, 4] and Directive n. 99/93/ES on a Community framework for electronic signatures respectively), while the Care for Health of the People Act is not expressly implementing any EU legislation. Therefore we believe that the more detailed analysis of the Care for Health of the People Act might reveal some more unique issues, which could eventually be interesting for example when considering if some new EU legislation in this area might be sensible.

To the Care for Health of the People Act an implementing n. 385/2006 Sb. Health Record Order (hereinafter referred as “Order”) has been later passed.

### 3 Electronic Health Records under the Care for Health of the People Act

The Care for Health of the People Act (that is its § 67a and following) is not defining the term “health record”. However, it at least states, what such a health record consists of. That is:

1. personal data of the patient in the scope necessary for identification of the patient and assessment of the anamnesis [5] (It is explicitly specified, that it can contain the birth certificate number of the patient.) and
2. information about the illness of the patient, about the process and results of examinations, treatments, and other significant circumstances related to the health state of the patient and the procedure during health care delivery.

#### 3.1 Three Possible Legal Ways of Having the Health Records in the Electronic Form

The Care for Health of the People Act expressly permits keeping the health record in electronic form (literally saying in its § 67b article 5 that, „Health record can be kept on a medium either in a text, graphical, or audio-visual form“.). It even allows for several ways how this can be done:

- (A) Health records can be first kept in paper form and the data from them transferred to the electronic form only later. In this case, it is not necessary to attach the advanced digital signature to the electronic variant of the record, but it is necessary to archive those former paper documents. This way even old records created before the switch to electronic health records can be transformed to the electronic form.

- (B) Health records can be first kept in the electronic form and then transformed to the paper. In such a case the person that made the record must also log the date on it and sign it and such a printout must be archived. The printout is considered a separate part of the health record (§ 67b article 6) and as such it must include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it (§ 67b article 3). In this case it is also not necessary to use the advanced digital signature.

- (C) Health records can be kept in the electronic form exclusively. In such a case the Act stipulates following rules:

- (a) All separate parts of the health record include the advanced electronic signature of the person that made the record,
- (b) safety copies of files are made at least once each working day,
- (c) after the expiration of the lifetime period of the record a transcript of the archival copies is secured,
- (d) the storage of archival copies that are made at least once a year is done in a way preventing additional changes to them.

#### 3.2 How to Apply These Rules to Different Types of Records

The question can be to what extent some of the mentioned rules (especially the rule to transform to the paper form under the alternative B and rules mentioned under alternative C) apply only to records in form of text and to what extent also to records in graphical or audio-visual form.

In practice these rules are not interpreted strictly. In our opinion though, it is necessary to apply the same rules as in the case of text records. That is, because the law is not talking about any differences and the opposite conclusion would be hardly acceptable, as it would in essence mean, that a document kept only in electronic form does not have to fulfil rules under alternative C. This should not be too hard to technically implement anyway, as from the point of the digital signature algorithms, there is essentially no difference between digital signing of text, picture or video (although with the larger data files it will obviously take more computing power to process).

The current legal state therefore seems such, that every graphical or audio-visual document about a patient in a digital form that is not going to be transferred to a paper form fall within the scope of the alternative C, that is, the rules concerning the backup procedures and usage of digital signature.

### 3.3 When to Apply the Advanced Electronic Signature

The Act stipulates, that every “separate part” of the health record must include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it, and, if health records are to be kept in the electronic form exclusively, all “separate parts” of the health record must also include the advanced electronic signature of the person that made the record. In this situation we found it necessary to consider the term “separate part of the health record” itself.

The law does not define it, but it can be inferred, that not every document in the health record must necessarily be signed by the advanced digital signature. Otherwise, the legislator would not use the term separate part of the health record, but it would link the rules directly to the term “record”. This conclusion is also supported by the wording of the implementing Order, which defines in its supplement n. 1 “the minimal content of the separate part of the health record”. This is not a list of parts of health record that are already separate, but instead of parts that might become separate (see § 3 article 2 of the Order) and for which special necessities are defined. In relation to these necessities the list is taxative, but as for the term separate part of the health record it is demonstrative. The point is, that every part of health record that is being detached, for example during its sending to another medical facility, should be signed by digital signature and marked with necessary identification data.

Such detaching and sending can be possible with virtually any kind of content of the health record (whether it is a X-ray picture or something else). For the fulfilment of the requirements it is enough if the document is signed with the digital signature (and the mentioned identification data are included in it) at the phase in which it is being sent (e. g. it is becoming separate). Of course though, that it must be the signature of the person responsible for the content of the document; if other person would be the one sending it, the signature of such a person would not be sufficient (see the wording “the electronic signature of the person that made the record”).

From this reason it seems more practical to have the documents in health record already signed right from their creation and not only when they have to be sent somewhere. Also the wider usage of digital signatures can be generally recommended, anyway, to improve credibility of the given system. Besides, for documents that are already stored in a way prescribed for separate parts of health record, it opens a way to consider the possibilities to exchange them in such a style that there would be no more necessary to send a request between medical facilities that someone must answer, but based upon a password and other security measures the system could evaluate the request itself and allow access to the data.

### 3.4 Concerning the Rules Related to the Archiving of the Data

Let’s have a look at other rules under the alternative C. Rules b) and d) should not cause, although their fulfilment will of course require some financial and other expenses, bigger legal or technical problems. Each work-day a backup of data must be made, during which all new records (e. g. new documents and changes of the older ones) must be archived compared to the previous backup (that must have been performed the day before). This rule will be of course fulfilled by usage of even higher standard, when all changes on one data-storage are immediately mirrored on another data-storage. Besides that, the law prescribes creation of additional backup of the records that must be performed at least once a year. In case of this backup, the storage must be done in a way preventing additional changes to them. As for the documents signed with digital signature this rule is, thanks to its attributes, fulfilled. The second option might be to use non-rewritable mediums (such as DVD-R). The question of eventual other ways and additional details how to store the data without the possibility of future changes to them the Act does not answer and leaves it to the individual subjects, or rather their employees, particularly the computing experts.

Significantly more difficult to analyse are the rules under letter c) “after the expiration of the lifetime period of the record a transcript of the archival copies is secured”. This provision seems rather unintelligible. Not only that it might not be clear to everybody what is “the lifetime period of the record”, but doubts arose also from the term “transcript” (if it is a copy, why the Act uses different word?), the term “archival copies” (which is the same expression as under letter d), but ordering, that is placement of rule c) higher, does not correspond to the sameness) and strange is the instruction to do it “after” (when the record is not, or might be not, readable anymore?!).

The intention of the lawmaker has probably been though, to set some standard of reliability for the data-storage of the health record. Therefore only such data-storage should be used, for which the lifetime period set by its manufacturer or provider has not yet expired, and a transfer to another data-storage ahead of such time must be done (Doing it “before” instead of “after” will not be a violation of the law - *argumentum a minori ad maius*).

This obligation logically relates primarily to the main backup, but considering the evident need to keep both backups usable, it seems fitting to apply it to them as well. In case of archival copies according to letter d) it is not necessary to infer this in such a way, as the Act deals with them specifically and somewhat more clearly. According to § 67b article 8 “While keeping archival copies of data on memory mediums of computer technology an access to the data and their readability (usability) must be guaranteed at least for the time prescribed for the archiving of health records”.

### 3.5 Other Formal Requirements

We already described some rules concerning what must be included as an information with health records, such as that each separate part of the health record must “include the personal data of the patient in the scope necessary for his/her identification and the specification of the medical facility that created it“. However, the Act, for all ways of keeping of the health record, prescribes some other rules that we should also mention at least briefly.

According to § 67b article 4 each record “must include date of its creation, identification and signature of the person that made the record. Corrections in health record are done by new record that must include date of its creation, identification and signature of the person that made the correction. The former record must stay readable“. A question might be, what is “the signature” according to this provision. In the context of the Act it is nevertheless clear, that the lawmaker meant only the paper version of health record and in case of electronic health record that does not have to include the advanced digital signature (variants A and B) it is apparently sufficient to list the person that made that record.

In the last quoted § we can note, that the records in electronic health record should not be completely erased, but an access to the corrected part must remain possible.

### 3.6 Right of the Patient to Access the Health Record

The Act after its amendment n. 111/2007 Sb. finally [6] introduces the right of the patient to access the health record (§ 67b article 12). In relationship with the topic of this article we would like to emphasize that in case of existence of electronic health records, the patient now obviously has the right to be provided with corresponding digital copy. The way to consider the possibilities of the on-line access to the health record by the patient himself opens too.

As a side note, we would like to remark that we would recommend to establish also the right of the patient to access the automatically generated logs about the access to the health record, which would future support their significant contribution to the protection of the records from unauthorized access.

## 4 Discussion and Conclusion

Above we described the core of the national legislation related to electronic health records and analysed the meaning and appropriate implementation of some parts of its text. We have found the current text of the Care for Health of the People Act to be sometimes problematic and inconsistent, and thus we believe that it should be rewritten to be clearer and more comprehensive. Nevertheless, as we could see, the legal framework in the Czech Republic indeed allows the usage of electronic health record,

which is the basic requirement for deployment of various e-Health applications.

What the authors of this article are finding concerning is what the Care for Health of the People Act does not say. The text of the Act is rather brief and obviously is not covering all aspects of implementation of electronic health records in detail. While we were talking about the Care for Health of the People Act we did not mention anything about any legally binding technical data standards set by law concerning the transfer of the digital data between different medical facilities. Neither had we talked about any legally created dedicated body entitled with establishing of such standards and policies (Such as the Office of the National Coordinator for Health Information Technology and the HIT Standards Committee in USA [7]). The reason is that there is no such a thing. There exists a certain standard called “Data Standard of Ministry of Health of the Czech Republic“, but this standard is not legally binding and despite its officially sounding name the Ministry of Health is letting it being developed mostly in an informal cooperation between various private companies. This standard is now widely used in the country, yet it is not accepted by all healthcare facilities, and the other problem is, that many of the facilities are using several years old versions of the standard, as they are not forced to update it, despite the authors of the standard are urging them to do so. Besides its problematic enforcement, we would also like to stress out, that it is a purely national standard, which does not even have any ambition [8] for compatibility with foreign facilities, e. g. to support transfers of electronic health records across the borders of the country. We believe this to be an issue, especially for a country that is a member of the ever more integrating European Union.

The briefness of the Act leaves a lot of the decisions related to the development of the e-Health applications up to the individual healthcare facilities. For example, as we could see, the Act sets rules as to when the advanced electronic signature has to be used; however, it does not set any detailed rules about the certification-service-provider. On one hand the usage of the advanced electronic signatures is mandatory, but on the other hand, it is not necessary for these signatures to be based on qualified certificates. Healthcare facilities thus might use a certification-service-provider that does not have any accreditation, or theoretically even create their own certification-service-provider. Obviously, such decisions are connected with responsibly towards the patients in case of some problems.

It might be argued, that it is actually a good thing, that the legal regulation sets only some basic rules to allow the existence of electronic health records and that is not too detailed, as the rapid development in the field of e-Health could in such a case quickly render the text of the statutes obsolete, and the too precise legal rules might limit the possibilities of development and deployment of various new technological solutions and services. The authors of this article are of such opinion though, that the Czech government should take more active role, and pro-

vide some more guidance in the processes we discussed, like in the area of creation and enforcement of interoperability standards.

## References

- [1] Stroetmann K. et al. European countries on their journey towards national eHealth infrastructures. Brussels: European Commission, Information Society Media Directorate-General, eHealth Strategies Report; 2011. Available from: [http://www.ehealth-strategies.eu/report/eHealth\\_Strategies\\_Final\\_Report\\_Web.pdf](http://www.ehealth-strategies.eu/report/eHealth_Strategies_Final_Report_Web.pdf).
- [2] Dostál Otto, Brechlerová Dagmar. Selected legal aspects of health records and telemedicine (in Czech). Prague: EuroMISE centrum; 2005.
- [3] Mates Pavel. Ochrana soukromí ve správním právu. Praha: Linde; 2004. In Czech.
- [4] Matoušová Miroslava, Hejlík Ladislav. Osobní údaje a jejich ochrana. Praha: ASPI Publishing; 2003. In Czech.
- [5] A diagnosis is reached by the examination of the patient. This consists in the obtaining of the history (anamnesis) and in the objective examination (status praesens). - Georg Klemperer. The Elements of clinical diagnosis. The Macmillan Co.; 1904. p. 1.
- [6] Buriánek Jan. Lékařské tajemství, zdravotnická dokumentace a související právní otázky. Praha: Linde; 2005. p. 54 and following. In Czech.
- [7] Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, § 2.A.III B.4.
- [8] Seiner Miroslav, Zámečník Miroslav. Současný vývoj a záměry rozvoje datového standardu MZ ČR. ISSN 1803-8115, p. 235-248. In Czech.