Digital signature of electronic dental records

Ivan Toshio Maruo & Hiroshi Maruo
Curitiba, Paraná, Brazil

**Introduction:** The purpose of this article is to examine the feasibility of digital signature technology to guarantee the legal validation of electronic dental records. **Methods:** The possible uses of digital signature technology, the actual use of digital signature technology to authenticate electronic dental records, the authentication of each part of the electronic dental record, the general legal principles involved, how to digitally sign electronic dental record files, and the limitations of this method are discussed. **Results and Conclusions:** It is possible to obtain electronic dental records that carry the same legal certainty as conventional, nonelectronic records. For this purpose, each part of the electronic dental records should be digitally signed by the author of the document. (Am J Orthod Dentofacial Orthop 2012;141:662-5)

Orthodontics is a dental specialty that deals with many technologic resources. Two-dimensional1 and 3-dimensional2-3 digital photographs, 3-dimensional digital dental casts,4,5 digital radiographs,6 computed tomography,7 3-dimensional cephalometry,8 and magnetic resonance imaging9 permit accurate diagnosis, planning, and treatment-result analysis. Furthermore, with scanners and digital cameras, we can digitize conventional, nonelectronic records and turn them into electronic records.10

Replacing conventional dental records with electronic records saves office space, facilitates access to patients’ medical and dental histories, integrates health care information, and helps to improve the quality of all health treatment. Simmons11 showed how electronic health and dental records will be part of American health professionals’ and patients’ routines within a few years.

However, the transition from conventional to digital must be managed carefully. Any digital file, including an electronic dental record, can be forged, raising doubts about its authenticity. Madhan and Gayathri12 demonstrated that digital photographs and radiographs can be manipulated, simulating clinical results that do not exist in the real world and forging images of patients’ records that seem to be real. Frequently, tampering is so well conducted that only a specialist can detect it.12

Because of the difficulty in demonstrating that electronic records represent something that really exists, their legal validity (ie, their integrity and authenticity) can be questioned in a judicial or an administrative lawsuit.

To guarantee the authenticity of digital medical images, Smith13 proposed the use of “digital signature technology.” Subsequently, Kobayashi and Furuie14 presented an algorithm to achieve viable integrity, authenticity, and verification on digital imaging and communications in medicine (Digital Imaging and Communications in Medicine) medical images, also using digital signatures.

The United States,15 Brazil,16 and the European Union17 regulate the use of digital signature technology, because electronic contracts are becoming common.

Surprisingly, although the system of digitally signing electronic health records was suggested in the United States,16 Brazil,14 Germany,19,20 Greece,21 and Taiwan,22 this subject is still largely unexplored for electronic dental records. We searched the PubMed database using the terms electronic dental records and digital signature, and found no articles.

The aim of this study was to examine the feasibility of digital signature technology to guarantee the legal validation of electronic dental records in a global perspective.

**POSSIBLE USES OF DIGITAL SIGNATURE TECHNOLOGY**

Digital signature means a mathematically generated mark using asymmetric key cryptography techniques that is unique to both the signatory and the information signed.15 For its implementation, a digital certificate (an electronic document that binds a person’s identity to his or her digital signature), a digital signature

---

1Private practice, Pontifical Catholic University of Paraná, Curitiba, Paraná, Brazil.

The authors report no commercial, proprietary, or financial interest in the products or companies described in this article.

Reprint requests to: Ivan Toshio Maruo, Rua Pasteur, 95, Bairro Batel, CEP 80250-080, Curitiba, Paraná, Brazil; e-mail, ivan_maruo@yahoo.com.br.

Submitted, revised and accepted, February 2012.

0889-5406/$36.00 Copyright © 2012 by the American Association of Orthodontists.

infrastructure (software, hardware, personnel resources, and the required procedures to effectively use digital certificates and digital signatures), and certification authorities (issuers of digital certificates) are needed.  

LEGAL PROCESS AND THE ACTUAL USE OF DIGITAL SIGNATURE TECHNOLOGY TO AUTHENTICATE ELECTRONIC DENTAL RECORDS

In Brazil, for example, the Brazilian Public Keys Infrastructure (ICP-Brasil) was created by a Provisional Executive Order in 2001. In 2006, the ICP-Brasil permitted the computerization of judicial processes, according to law number 11419/2006, in which only digital documents are used. In 2007, the Brazilian Federal Board of Medicine approved the technical standards of medical records digitizing and permitted the elimination of conventional records if ICP-Brasil digital certificates to digitally sign the files were used.

Documents are admissible in court as long as they are relevant. A relevant document is one that tends to make a material fact more or less likely than it would have been without the document. If a dentist or a physician is a defendant in a liability lawsuit, the patient’s health records are relevant documents.

In law, the relevant documents are referred to as evidence. In the United States, federal courts adhere to the Federal Rules of Evidence, which determine what type of evidence is admissible and in what situations. In Brazil, for example, the Brazilian Public Keys Infrastructure guarantees to the electronic records the same legal status, opinion, or diagnosis. So, if each part of the electronic dental record is digitally signed by its author, all of the electronic dental records are considered to be authentic.

GENERAL LEGAL PRINCIPLES

The efficiency of the digital signature technology to legally validate electronic dental records can be questioned, because manipulated digital files can be digitally signed after forgery.

To elucidate this matter, it is important to understand that certain values comprise a common foundation among western legal systems, and these values are expressed by the general principles of law. Two of these principles must be analyzed in the case of digital signatures of electronic dental records: the good-faith principle and the burden-of-proof principle.

GOOD-FAITH PRINCIPLE

The good-faith principle means that the parties in a transaction must deal honestly and fairly with each other, represent their motives and purposes truthfully, and refrain from taking unfair advantage that might result from a literal and unintended interpretation of the agreement between them.

So, respecting the good-faith principle, it is assumed that health care professionals and patients are honest, and there is no reason for digitally signing health records that do not correspond to reality.

Actually, it is the same reasoning that is applied to conventional nonelectronic records. Because of the good-faith principle, when complementary examinations are made by a radiology laboratory, the health care professional considers them to be authentic without asking for proof.

It means that the digital signature technology does not guarantee absolute authenticity of electronic health and dental records. In fact, digital signature technology guarantees to the electronic records the same legal validity as the conventional nonelectronic ones.

BURDEN OF PROOF PRINCIPLE

When the authenticity of electronic dental records and conventional nonelectronic dental records is questioned, the burden-of-proof principle is used. It means that enough evidence must be introduced before the jury or other tribunal.

Each country might treat differently the issue of the burden of proof, but the general rule is that the person who affirms something must prove it. When something is alleged and not proved, the court considers that what was claimed is untrue.
For example, in the Brazilian legal system, when there is doubt concerning the authenticity of documents, the court will apply the burden-of-proof principle, laid down in article 333 of the Civil Process Code:

1. The burden of proof rests (1) with the plaintiff, in relation to the constitutive fact of his or her right; and
2. (2) with the defendant, in relation to the existence of the impeditive, amending, or extinctive fact of the plaintiff’s right.

Because digital signature technology is usually regulated by government laws, there is no reason to deviate from this rule. It means that the person who questions the authenticity of an electronic or a nonelectronic document must prove that it has been forged.

Because of the good-faith principle, although the authenticity of electronic and nonelectronic documents can be questioned in a lawsuit, the person who digitally signs a file guarantees that it is not forged. In addition, because of the burden-of-proof principle, signed documents are assumed to be authentic until proven otherwise.

**DIGITALLY SIGNING ELECTRONIC DENTAL RECORDS FILES**

A digital signature is a method for ensuring the integrity of a message or document, authenticating the identity of the signer, and establishing nonrepudiation of the signature. This is possible because only the authenticated signer could have created the digital signature that is attached to the document.

To sign digital files, a person must purchase a *private key* (which is saved in either smart cards or tokens) bound to a *public key*. The public key is issued by a certification authority (a trusted third party) and is available for verification but cannot be used to sign new documents.

When a digital signer software, such as BRy Signer (BRy Tecnologia S. A., Florianópolis, Brazil), is used, the file is encrypted with both the private key and the public key. The software can both sign digital files and check the digital signature of previously signed files.

The Figure illustrates how the digital signer software checks the digital signature of a digital file. The signer’s personal data, the digital signature validation, and the time of the file signature are shown by this software.

**LIMITATIONS OF THIS METHOD**

The limitation for the immediate implementation of this proposal for the legal validation of electronic dental records is the necessity of the dentist’s, the radiology laboratory’s, and the patient’s digital certifications.

However, this limitation is momentary, because digital signature technology is improving and being used in many countries.

Soon, every citizen will have a digital signature. From now on, this proposal for the legal validation of electronic dental records will be available to all professionals.
CONCLUSIONS

It is possible to obtain electronic dental records that carry the same legal certainty as conventional nonelectronic records. For this purpose, each part of the electronic dental record should be digitally signed by its author.

REFERENCES

11. Simmons KE. Electronic medical record and its implications for or- thodontic records. For this purpose, each part of the electronic dental record should be digitally signed by its author.