MEDINFO 2007
HISA Ltd Australia
© 2007 The authors. All rights reserved.

The Brazilian Healthcare Software Certification Process

Beatriz F Leão[a], Cláudio G A Costa[b], Lincoln A Moura Jr[a], Roberto A. D'Avila[c]

[a]*VIDATIS – Health Information Systems, São Paulo, Brazil*
[b]*São Paulo City Department of Health, SãoPaulo, Brazil*
[c]*Federal Medical Council, Brasília, Brazil*

Abstract

This paper describes the Brazilian Healthcare Software Certification Process started in 2004. The Brazilian Health Informatics Society (SBIS) and the Federal Medical Council (CFM) have proposed and are conducting the certification process. This paper describes the motivation, the history, the three phases methodology adopted, and its current status. A comparison with other international initiatives of health information systems certification is also presented. To conclude the future plans are presented.

Keywords:

healthcare information systems, standards,
software certification

Introduction

The use of computerized systems in medical offices is increasing worldwide. Brazil has a long tradition of using IT in healthcare. The Brazilian National Health System - SUS adopts electronic standards for hospital and outpatient billing for more than 25 years. All information is available for consultation at the Ministry of Health homepage (www.datasus.gov.br) [1]. More recently, the National Regulatory Agency for Supplementary Health – ANS, responsible for the regulation of the private market, has published TISS, an electronic messaging standard, based on XML schemes, to send billing information to and fro healthcare providers and payers. From May 2007 on, the standard TISS becomes mandatory[2]. There is a national registry with unique identifiers for persons (so far with 116 million persons uniquely identified), healthcare providers (149 thousand) and healthcare workers (1.5 million)[3]. A national PKI (public key infrastructure) - ICP Brasil, based on open standards, gives legal validity to documents digitally signed, ever since 2002[4]. Brazil as well as Mexico is the two countries where the number of Internet hosts grows more in the world according to recent publications [5].

Motivation

Many of the hospitals and large clinics, at least in the larger cities already use health information systems, mostly for billing and patient record purposes. These organizations face the ever growing problem of storing the paper medical record. According to the Brazilian Federal Research Council it is mandatory to store the paper medical record for at least 20 years after the patient's last visit to the healthcare unit. At the same time, physicians in their medical offices are largely using electronic heath records systems. Some of these physician offices, regardless of the regulations, are paperless. As the regulations and legal validity of electronically signed documents evolved in the Country, several physicians motioned their Regional Medical Councils, looking for legal advice on whether they could become paperless. The Regional Medical Councils (there is one for each of the 26 Brazilian States) did not feel comfortable in replying and sent all those requests to the Federal Medical Council, which, in turn, decided to create a specific Technical Committee on Health Informatics and Telemedicine to, with the support of the Brazilian Health Informatics Society (SBIS) try to answer to those questions.

In 2002, due to the large number of requests from the Brazilian healthcare community, CFM and SBIS established a cooperation agreement to define and implement a software certification process that would allow, in the long run, for physicians and healthcare providers to be paperless safely and legally, according to the Brazilian regulations.

The next sections describe the methodology adopted in the certification process, the present status, lessons learned and future plans.

The Certification Methodology

Once the legal aspects of the agreement were established the technical group started to work. By 2002, there was no other international experience of software certification for healthcare, more precisely for systems that dealt with patient identified health information. The Certification Commission for Healthcare Information Technology (CCHIT) was created by the US government only in 2004 and is today a very successful example of healthcare software certification [6].

Legal background

In order to understand what we were dealing with, an extensive bibliographic review on software certification,

as well as on the Brazilian regulations for digital signatures, information security, privacy and confidentiality issues was carried out. In addition to that, the work of the ISO-TC 215 Health Informatics Committee was taken as a prime reference. As our understanding evolved, so were evolving the two basic documents we have used as references for the architecture, content, structure and function requirements of the certification process: ISO/TS 18308:2004 - Health informatics - Requirements for an electronic health record architecture [7] and the ISO/TR 20514:2005 Health informatics -- Electronic health record -Definition, scope and context [8].

The Federal Research Council published, in 2002, two specific regulations on patient records – Resolution CFM 1638/2002, and on electronic health record systems – CFM 1639/2002 [9,10]. These two resolutions together with the ISO-TC 215 documents above mentioned, and the ISO/IEC 17799:2005 Code of Practice for information security management [11] were the key documents used to define the SBIS-CFM certification process.

CFM 1638/2002 resolution defines the patient record as a document that contains text, images and signals related to the patient and that the resulting set of items is a private and confidential piece of information that can only be shared for patient care purposes. According to the Brazilian legislation, all information on the patient belongs to the patient. Physicians in their offices and health care providers in general have the obligation of keeping patient files for a period of at least 20 years (for the paper record). The 1638/2002 resolution also details the minimum content of the patient record. The recommendation is that the patient record (no matter whether electronic or on paper) has to contain the patient identification (it recommends the use of the national person identification registry), patient history, physical examination, ancillary tests and its results, therapeutics planning, diagnoses, evolution, surgical reports (if the case), and all medical orders. Summary discharges in case of hospital admissions with clear patient's recommendations in lay language. If on paper, it's mandatory that all documents be legible and signed by the attending physician. If electronic, the documents must be digitally signed according to the Brazilian PKI otherwise they must be printed and hand signed. The 1638/2002 resolution also deals with exceptions, as when the patient cannot speak, in which case it describes in detail what information has to be written on the patient file.

The 1639/2002 CFM was published a month after the 1638 in August 2002. It establishes the foundations of the SBIS/CFM certification process and describes the first set of technical recommendations for the process. These first recommendations were expanded in a full publication: The EHR systems security, content, and functionality requirements for the SBIS/CFM certification process, as described in the following sections. Among the recommendations, it says that for those who decide to use electronic health records, files must be saved forever, which means to the actual technology limit and that proper mechanisms should be granted to guarantee the compatibility of the storage devices, as technology evolves. That is also a recommendation present in the ISO/IEC 17799:2005 regulations. In addition to that, it is also recommends, and makes it mandatory for those who will have adopted the EHR, the existence of a Patient File Committee. The Head of this Committee is the one legally responsible for the patients file and for keeping its privacy and confidentiality. Should any legal problem occur, this is the person that is going to be implicated. The two resolutions made it clear to the healthcare community that it was possible to move to the paperless environment but it is necessary to improve drastically specially the small offices' *so called* "EHR" systems. Many physicians were already unable to defend themselves in malpractice suits because all they could present to the court was a paper printed from a simple system with no guarantee whatsoever that the specific piece of information was valid.

SBIS-CFM certification scope

Software certification is a rather complex task. It demands that at least two main issues are taken into account: the software product itself and its use in different organizations. For example, the same software product may be complaint with security requirements in one site, while not in others, because users share passwords, for instance. This has to do with the software utilization, rather than with the software product itself.

It was decided that the SBIS/CFM certification scope target any software product that captures, stores, manages, publishes or electronically communicates patient-identified health information, or, in other words, is an EHR. This definition is on purpose similar to the ones described in the ISO TC 215 aforementioned documents [7,8].

It was also decided that the SBIS/CFM certification is a VOLUNTEER process, meaning that only organizations that want to become paperless have to be certified. Recently the Federal Regulatory Agency for Supplementary Health, in its publication of the electronic standard for exchanging billing information, recommended that all systems implementing the communication should be compliant with at least Level 1 Security SBIS/CFM, as explained ahead.

SBIS/CFM certification phases

The SBIS/CFM certification process is composed of two basic phases: Phase 1 – Compliance Declaration; Phase 2 – Auditing and Quality Labeling. A third phase has also been envisioned in which necessarily the Ministry of

Health and ANVISA, the Brazilian Health Surveillance Agency will have to participate.

A Manual with all the Security, Content, Structure and Function Requirements for EHR was elaborated and went into public consultation in 2003, through the Internet[12]. The market reacted promptly considering the requirements too hard. The decision was then to split the process in three phases, based on the need to start with a lighter, educational phase, in which the main objective was to let the market, in special the small players, understand what the requirements were and have enough time to adapt. Brazil IT healthcare market mimics what the healthcare market is: many scattered small players attending the local market. There has always been the concern not to kill the local initiative, but rather to qualify it and make the world of standards, privacy, confidentiality and PKY for digital signature fully understandable even for the very small companies that offer "EHR" systems for the local physicians in the small communities across the country.

Since it had also and educational purpose, the Manual includes a large introduction with references to the CFM resolutions, ISO TC 215 documents, ISO 17799 Security Code of Practice and ICP-Brasil, the Brazilian PKY Infrastructure. The EHR system requirements are divided into the following sections: Security, Content, Structure and Functionality.

The Security chapter is based on the ISO/IEC 17799:2005 Code of Practice for information security management and in the privacy and confidentiality rules of the CFM Ethical Code of Practice. According to the Manual, EHR systems can be classified as Guarantee Security Level 1 or Level 2. The difference is that to be classified as Guarantee Security Level 2, the EHR system has to be compliant with all Level 1 requirements **and** provide digital signature authentication based on the ICP-Brasil.

The Content, Structure and Functionality requirements are an adaptation from the ISO-TC 215 documents. Every requirement is identified as mandatory or optional. Some are identified as "desirable", as is the case of the need to incorporate comments in any data entry or to specify the relevance level of the information. The "desirable" attribute indicates to the community that although not mandatory today, this is an attribute that will probably be mandatory in the near future.

Each requirement is uniquely identified within the Manual, has a description and a reference to the information source. All national standards for patient, healthcare provider and healthcare worker identification and description are part of the mandatory requirements of the Content Section.

Phase I – Compliance declaration

Phase I of the SBIS/CFM Certification Process is FREE and totally online by accessing SBIS's website (www.sbis.org.br). It consists of a self-proclaimed declaration from the software supplier, stating that the specific product registered at SBIS website is compliant with the Requirements Manual at the Security Level 1 or 2.

The process is simple and straightforward as depicted in Figure 1 below.

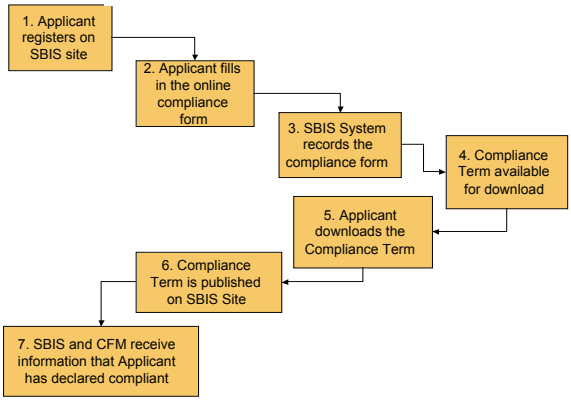

Figure 1 - SBIS-CFM Certification Process – Phase 1

The applicant is the software supplier. It may be a company, an academic institution or even a single person. The first step is the registration of the organization or person responsible for the software product. A brief description of the product is also required, such as operational system used, architecture, category (hospital, outpatient, medical office, laboratory, imaging, public health integrated system, billing). After that, the requirements are presented as a questionnaire to the applicant, to be answered on-line, as shows Figure 2 below. When finished, if all the mandatory requirements are present, the compliance declaration is published at the web site and can be downloaded by the applicant.

Questionário Certificação SBIS-CFM - Microsoft Internet Explorer

Certificação SBIS-CFM

Fase I

Questionário para Declaração de Conformidade

Empresa : Empresa Teste S/A

Produto : Sistema Exemplo de Certificação

Nível de Segurança : NGS1

Marque somente aqueles requisitos que o produto (sistema/software) atender integralmente

Ao terminar de responder o questionário, clique em : Salvar Cancelar

Requisito		Descrição
RSEG		Requisitos de Segurança para Sistemas de RES
RSEGM1		Controle de versão do software
☐	RSEG1.1	Possuir versão do software associada a uma referência (nome, fabricante e número de versão) única e não ambígua
☐	RSEG1.2	A versão do software deve ser marcada e com marcação igual constante em seu código fonte, possibilitando a rastreabilidade dos fontes que o geraram
RSEGM2		Autenticação e Controle de acesso
☐	RSEGM2.1	Possuir mecanismo de administração de usuários ligados a um administrador do SRES e/ou banco de dados
☐	RSEGM2.2	Implementar os mecanismos necessários para a estabelecer a política de controle de acesso através da definição de perfis e/ou grupos, baseados nos diferentes papéis da área de saúde. Considerar que um mesmo usuário pode ter mais de um papel com diferentes permissões de uso

Figure 2 - SBIS/CFM Certification Questionnaire

Phase 1 is an educational phase for the market. Neither SBIS nor CFM takes any responsibility on what has been declared. Therefore it's not recommended to become paperless based on this compliance term.

Phase II Auditing – SBIS/CFM quality labeling

The second phase of SBIS/CFM certification process is also a volunteer one, but not without costs, since here there is the need to pay for the systems auditing.

In Phase II, all systems compliant after Phase I can proceed to Phase II and be audited by accredited organizations. The process is also simple and mostly done through the Internet as in Figure 3.

The applicant chooses the accredited certification organization, through by assessing the company's history and available auditors. Each auditor's biography is available, as well as their declaration of interest. The objective here is to have full transparency, avoiding possible conflicts of interest.

The applicant has to approve the commercial proposal for the auditing which triggers the start of the auditing process. The auditing process is objective, with the auditors (always two) having to follow very detailed script and case tests, to check the system compliance with each Manual Requirement.

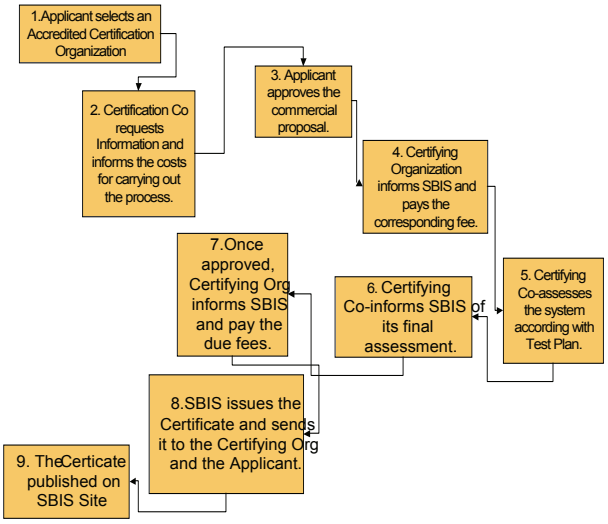

Figure 3 - SBIS-CFM Certification Process - Phase 2

Once the auditing has finished, SBIS receives the report from the accredited certification organization and, should the system be compliant, a Quality labeling is issued to the applicant and the associated certificate is published on SBIS website.

Phase III – Ministry of Health involvement

Phase III necessarily requires that the Brazilian Ministry of Health and ANVISA, the Brazilian Health Surveillance Agency, take part in the process, as those are the organisms with legal power to legislate on these matters. CFM has power over medical doctors. The Ministry of Health and ANVISA have power over all healthcare organizations. Nevertheless, Phase III deals with certification of products and their "on site" implementation. Systems that have survived Phase II are natural candidates for Phase III. Assessing how systems perform after implementation is a more complex process that relates to ISO 9000 series of certificates, and SBIS/CFM must learn from there.

Results

The SBIS/CFM Requirements Manual was first published in February 2004. Phase I of the certification process is operational since October 2004. More than 200 software developers have registered on SBIS website and have downloaded the SBIS/CFM Requirements Manual.

At the moment (December 2006), fifty one (51) software products have self-proclaimed compliance with the Manual. Products are divided in categories, according to the table bellow.

Table 1 – Categories of software compliant to SBIS/CFM requirements

Category	Number of products conformant
Public Health Systems	6
Medical office automation / EHR	17
Billing – health insurance	7
Medical Images	3
Occupational Health / Surveillance	4
Hospital Information Systems	14
Total	**51**

Present status

At the moment, the documents to initiate Phase II are ready: the Auditor Manual with all the scripts and case tests, the Code of Ethics for the auditor and the Term of Reference to accredit Certification Organizations. The training program for the auditors is scheduled for January 2007 and it is our intention to have Phase II operational by March 2007. Hopefully by MEDINFO we will have the first results of Phase II to show.

Conclusions

Certifying software is a very complicated and costly task. The Brazilian process had to start in small steps to accommodate and educate the market. Today there is a consensus that the process will qualify the software suppliers in Brazil and will allow for a secure transition to a paperless environment.

The Ministry of Health participation in this process is desirable since this would guarantee greater investment in the process. So far the work has been sponsored solely by the Brazilian Federal Council.

References

[1] IDB – Indicadores e Dados Básicos Brasil 2005 - http://tabnet.datasus.gov.br/cgi/idb2005/matriz.htm

[2] ANS / MS. Resolução Normativa 114. Outubro de 2005. Downloaded December 4,2006 at: http://www.ans.gov.br/portal/site/_hotsite_tiss/pdf/rn114.pdf

[3] Lemos M, Leão BF. Standards adopted in the Brazilian National Health Card Project. IN: Proceedings of the 8th Conference on Nursing Informatics, Rio de Janeiro, June 2003.

[4] ICP-Brasil**.** Captured in 10/12/2003. Online. Available at: http://www.icpbrasil.gov.br

[5] Chinn M, Fairlie R. ICT Use in the Developing World: An Analysis of Differences in Computer and Internet Penetration. Available online PDF [40p.] at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=936474

[6] Certification Commission for Healthcare Information Technology (CCHIT) Organizational Structure. Online. http://www.cchit.org/about/organization/

[7] ISO/TS 18308 - Health informatics -- Requirements for an electronic health record architecture http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33397

[8] ISO/TR 20514:2005 Health informatics -- Electronic health record -- Definition, scope and context http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39525&COMMID=&scopelist=

[9] CFM. Resolução 1638/2002. Captured on August 25,2003. Available at: http://www.cfm.org.br.

[10] CFM. Resolução 1639/2002. Captured on August 25, 2003. Available at: http://www.cfm.org.br.

[11] ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management Available at: http://www.iso.org/iso/en/prodsservices/popstds/informationsecurity.html

[12] SBIS-CFM. Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES). Brasília-DF, 2004.

Address for correspondence

Beatriz de Faria Leão, MD, PhD
Email: bfleao@terra.com.br
Phone:+55-11-8114-1617