Applying a Presentation Content Manifest for Signing Clinical Documents

Chung-Yueh Lien,¹ Chia-Hung Hsiao,² Lu-Chou Huang,¹ and Tsair Kao³

In this paper, we demonstrate how to digitally sign a content manifest of a presentable clinical document that contains multiple clinical data with presentations. Only one signature is needed for an entire clinical document with multiple data resources, which can reduce the computation time during signing and verifying processes. In the radiology field, a report may contain text descriptions, images, and annotations that are stored separately in different data resources. The manifest signature would be a proper means for integrity checking for all the clinical data within the manifest. The manifest signature can be extended with a trusted third party to add a digital time signature for long-term verifiability. The performance of the manifest signing compared with that of a traditional digital signing was evaluated. The new manifest signature can be used for signing different types of presentable clinical documents, such as HL7 CDA documents and DICOM image reports.

KEY WORDS: Security, digital signature, electronic health record (EHR), digital imaging and communication in medicine (DICOM)

INTRODUCTION

Several digital signature mechanisms have been developed, and most of them are based on public key cryptography under public key infrastructure (PKI) environment.¹ In order to implement the digital signature of electronic health records (EHR), some issues should be of concern, including integrity, authenticity, and long-term verifiability.^{2,3} The digital signature specifications in the radiology domain have been addressed by Digital Imaging and Communication in Medicine (DICOM)⁴, Health Level 7 (HL7), and Integrating the Healthcare Enterprise (IHE).⁵ In the real world, an EHR may contain many different types of clinical data (text, image, waveform, etc.). For example, a radiology report may contain DICOM-

formatted images and presentation states with diagnostic reports (HL7 Clinical Document Architecture (CDA)⁶ or DICOM PDF (Portable Document Format)⁷ format). The HL7 CDA is a document markup standard that specifies the structure and semantics of clinical documents as the Extensible Markup Language (XML) format for the purpose of exchange. DICOM PDF includes source DICOM image files as PDF attachments by a user-defined XML Forms Architecture (XFA).⁸

If the existing electronic signature standards are followed, the integration of different standards will cause lots of trouble when signing and verifying the signatures.⁹ Hollerbach et al. analyzed the different data formats in health care for conclusive and secure long-term archiving. They mentioned the lack of stability of data formats and also the heterogeneity of integration in the clinical field.¹⁰ On the other hand, DICOM only regulates the digital signature for single image and does not offer a suitable solution for multiple resources. A legal signed DICOM file must contain one digest

¹From the Institute of Biomedical Engineering, National Yang-Ming University, Taipei, Taiwan.

²From the Department of Medical Informatics, Tzu Chi University, Hualien City, Taiwan.

³From the Department of Biomedical Engineering, Hungkuang University, 34 Chung-Chie Rd, Shalu, Taichung, 443, Taiwan.

Correspondence to: Tsair Kao, Department of Biomedical Engineering, Hungkuang University, 34 Chung-Chie Rd, Shalu, Taichung, 443, Taiwan; tel: +886-4-26318652; fax: +886-4-26313871; e-mail: tskao@sunrise.hk.edu.tw

Copyright © 2009 by Society for Imaging Informatics in Medicine

Online publication 17 March 2009

doi: 10.1007/s10278-009-9191-y

and one digital signature. If a study contains hundreds of DICOM files or the Structure Report (SR) references many DICOM images, then the same number of digital signature is required. However, it is impractical to implement these lengthy signing and verifying processes in the real world due to high computation time demands. The implementation of DICOM-specified signature still has performance problems due to file numbers and huge file sizes.^{11,12}

Digital Signatures

The integrity and authenticity of digital data can be validated using a digital signature mechanism. A digest of the digital document is calculated from an irreversible one-way hash function. Hash checking of digital data is commonly used on the Internet to prevent unauthorized modification. The digital signature can be implemented by a combination of the hash algorithm and public-key cryptography such as the RSA (Rivest-Shamir-Adleman) algorithm¹³ to reduce the complexity of calculations. When RSA algorithm is used to calculate a digital signature, the signer encrypts the digest of the digital document with his/her own private key. The recipient with access to the public key of the signer may verify the digital signature. The security of the RSA algorithm is based on the difficulty of factoring large integers. Some studies have proposed digital signature mechanisms to provide the authenticity and integrity of clinical data in the radiology field.^{14–16} Under PKI, it is possible to work with the certificate and a trusted third party (TTP) to process inter-institutional applications and achieve the long-term verifiability of EHR.¹⁷ Digital signatures are authorized for the clinical data to be accepted as the replacement for paper-based records.

Manifest Signature Mechanism

IHE adopts XML Advanced Electronic Signatures (XAdES) for signing and verifying clinical documents (either XML or non-XML data).⁵ XAdES is based on World Wide Web Consortium (W3C) XML Signature with XML-extended attributes for long-term verifications. The W3C XML Signature provides two mechanisms to sign multiple data resources: manifest signature and multi-

ple signatures. In the first mechanism, the digest of each data resource is obtained, and the manifest consists of a list of digests. Only one signature is created from signing this manifest, and the signature with the manifest would be a proper means for integrity check for all the clinical data within this signed manifest. In the second mechanism, the multiple signatures are applied to a large number of documents. Each signature represents the specific data resource, as DICOM has suggested.

Inconsistent Presentation of EHR

Many clinical documents are presented in specific application, such as using a browser to present HL7 CDA data with Extensible Stylesheet Language Transformations (XSLT), which transforms the XML formatted document to HTML using a predefined XSLT style sheet¹⁸, or a DICOM viewer to display DICOM image with corresponding presentation objects. For example, if only the CDA document is signed, and not the XSLT style sheet, inconsistent presentation of CDA document will occur. The principle of implementing the electronic signature (both traditional digital signature and manifest signature) for presentable documents does not sign only the clinical data but also presentation.¹⁹ The signing range should contain all of the data related to the clinical data. If there is only signing of clinical data, incorrect or ambiguous display could happen when presenting the clinical document between the signer and the receiver.^{20–22} Unfortunately, the manifest signature in IHE and W3C specifications does not clearly identify what presentation documents should be signed.

In this paper, we propose a new manifest signature architecture modified from IHE specifications to digitally sign the clinical data with its presentation. Only one signature represents the signature for an entire clinical document with multiple data, which can reduce the computation time during signing and verifying processes. We can clearly identify and manage the clinical documents that are signed in the content manifest. Based on previous work^{23,24}, we demonstrate how to use the content manifest for handling presentable radiology reports (CDA documents, DICOM objects, and HTML web pages) that are stored in a medical image content repository.

Fig 1. Manifest-generating process.

METHODS

Proposed Manifest Architecture

The new manifest modified from the Sharable Content Object Reference Model (SCORM)²⁵ is used to define and access the resources. The proposed manifest-generating process is shown in Figure 1. The new manifest structure contains three parts: metadata M , organizations O_{RG} , and resources R_S . M is used to facilitate the discovery

of the documents for exchange by following the IHE Cross-Enterprise Document Sharing (XDS) profile. O_{RG} is used to define and manage the documents in the manifest. R_S provides an index of all documents to query and retrieve by a resource mapping.

In the manifest, there are N documents, $D_1, D_2, \dots, D_N$, needing to be signed. For each reference, $\text{Ref}(D_k) = \text{ID}(D_k) \wedge H(D_k)$ is calculated. The symbol “ $\wedge$ ” means cascade. $\text{Ref}(D_k)$ represents the reference of D_k . Information related

```

----- Reference Type of DICOM Data Object -----
- <Reference URI="1.2.840.XXXXX.XXXX.XXX.XXXX.20080313.112659875_1.dcm" type="DCM">
  <DigestValue>bLKurFguHwcWyHTAh43a8A==</DigestValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
- <Transforms>
  <Transform Algorithm="urn:oid:1.2.840.10008.1.2.1" />
</Transforms>
</Reference>
----- Reference Type of JPG Format -----
- <Reference URI="MR^HEAD AND GAD - aMRI HEAD (REPEAT SCAN)_0001.jpg" type="Presentation_Stata">
  <DigestValue>RYKHx+EMGUSOFptK+RRCaQ==</DigestValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
- <Transforms>
  <Transform Algorithm="MIME/JPG" />
</Transforms>
</Reference>
----- Reference Type of XML Format -----
- <Reference URI="CDA_Report.xml" type="xml">
  <DigestValue>BcHiBuDDvysnjA/HTcjT0A==</DigestValue>
  <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
- <Transforms>
  <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments" />
</Transforms>
</Reference>

```

Fig 2. An example of reference types of data formats. This example shows three reference types of $\text{Ref}(D_k)$: DICOM data object, JPG image, and XML data. The value of “Transform Algorithm” means canonicalization, which is a process for converting XML data into a “standard” canonical representation.

Fig 3. Digital signing and retrieving digital time signature process.

to D_k is defined in $ID(D_k)$, which describes the identifier and transform algorithm used. $H(D_k)$ is the hash value of D_k , where H is a hash function such as Message-Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 (SHA1), etc. The

reference can provide document with well authenticated and authored and can check the identity of the author and authenticator of each document. The resources R_S , constructed by cascading N number of $\text{Ref}(D_k)$, is defined as follows:

$$R_S = \text{Ref}(D_1) \wedge \text{Ref}(D_2) \wedge \dots \wedge \text{Ref}(D_N) \quad (1)$$

Figure 2 shows three examples of $\text{Ref}(D_k)$ for different data types presented as XML. In Figure 2, the value in $\langle \text{Transform Algorithm} \rangle$ of the DICOM data object type is urn:oid:1.2.840.10008.1.2.1, which expresses the explicit little endian coding for DICOM; this attribute can deal with different data formats. In addition, it

Diagnostic Imaging Report - Windows Internet Explorer

C:\Documents and Settings\TKao\Desktop\Paper\Manifest\DEMO\Index.htm

Diagnostic Imaging Report

*****附設醫院***** Hospital

患者姓名 (Name)	*****	性別年齡 (Sex and Age)	男 43 歲	入院日期 (Admission Date)	2006/06/23
病歷號碼 (ID)	*****	出生日期 (Birth Date)	****/**/****	收治科別 (department)	鼻科 (Nose) --> 放射治療 (RT)

入院診斷: (Diagnosis on Admission)

1. Nasopharyngeal carcinoma, non-keratinizing, cT1N3M0
2. Alcoholism

出院診斷: (Diagnosis on Discharge)

1. Nasopharyngeal carcinoma, non-keratinizing, cT1N3M0, s/p port-A insertion and preparation
2. Alcoholism

主訴: (Chief Complaint)

Left neck mass noted for about 5 weeks

病史: (History)

This 43 y/o male was quite well before. Around 2006/05, left neck mass was found and he went to our OPD. no hearing impairment were noted. Physical examination revealed about 8 cm firm mass over left level II area and 2 cm mass over left level V area. nasopharynx area was noted. Biopsy was done and it revealed non-keratinizing carcinoma. Under the microscope...

Diagnostic Imaging Report

Patient: ***** **MRN:** 4030012

Birthdate: January 1, 1922 **Sex:** Male

Consultant: ***** MD **Created On:** July 10, 2006

RADIOLOGY STUDY OBSERVATION (Findings)

Magnetic resonance imaging of head and neck before and after intravenous gadolinium injection was performed with the following pulse sequences: axial spin echo (SE) T1W, axial fast spin echo (FSE) T2W and post-contrast axial, coronal fat-saturation SE T1W:

asymmetrical increase thickness of nasopharyngeal wall with left side thicker than the right side. extensive bilateral level II and level V and left retropharyngeal lymphadenopathy. negative study of examined brain and skull base.

Conclusions

asymmetrical increase thickness of nasopharyngeal wall with left side thicker than the right side with extensive bilateral level II and level V and left retropharyngeal lymphadenopathy, compatible with NPC although the primary tumor is disproportionately small.

Fig 4. The display of a radiology report on a web browser. This radiology report includes discharge note, diagnostic image report, and image results. In this 43-year-old male, an 8-cm firm mass was found over the left level II area and a 2-cm mass over the left level V area. Irregular surface over left nasopharynx area was noted. Magnetic resonance imaging of head and neck before and after intravenous gadolinium injection was performed. All records were de-identified before disclosure.

can be extended for multiple data formats defined by the user. We reconstructed the reference of metadata $\text{Ref}(M)$, organizations O_{RG} , and R_s as the manifest M_D , defined as:

$$M_D = \text{Ref}(M) \wedge O_{RG} \wedge R_s \quad (2)$$

Signing Process

The signing process is shown in Figure 3. Based on the RSA digital signature algorithm, using the

signer's private key P_r to encrypt $H(M_D)$, the digest value of M_D , as the digital signature $DS(M_D)$, we then defined the digital signature process as

$$DS(M_D) = \text{SIG}(P_r, H(M_D)), \quad (3)$$

where SIG is the signing process. The $H(DS(M_D))$ is calculated and sent to the time stamp authority (TSA). The TSA concatenates a timestamp T_{SS} to the $H(DS(M_D))$ and calculates the hash of this concatenation as $H(H(DS(M_D))||T_{SS})$. The symbol

Fig 5. An example of manifest structure of a radiology report presented as XML. The discharge note, diagnostic image report, image results, and DICOMDIR are managed by O_{RG} using Items, Item001 to Item004, respectively. Each Item refers to the data in the R_s using the attribute *identifierref*: Src001 to Src004. For example, Item004 of O_{RG} represents the DICOMDIR, and the images are mapped from *<resource identifier="Src004">* in the R_s .

“||” represents the concatenation process, and T_{SS} is the Greenwich Mean Time (GMT) timestamp which confirms the synchronized time. The $H(H(DS(M_D))||T_{SS})$ is encrypted by P_{rTSA} , which is the TSA’s private key as the qualified digital time signature TSA_{SIG} defined as:

$$TSA_{SIG} = \text{SIG}(P_{rTSA}, H(H(DS(M_D))||T_{SS})) \quad (4)$$

Performance Analysis

Assume the times required for hashing, signing, and digital time signature retrieval for document n are T_n , T_r , and S_n , respectively, where $1 \leq n \leq N$. The signing time T_r is the same for each document. Since the timestamp retrieval time depends on the network status, here S_n is just for reference. If we create digital signature for each document one by one, the total calculation time is

$$T_{\text{total-trad}} = \sum_{n=1}^N T_n + N \times T_r + \sum_{n=1}^N S_n \quad (5)$$

However, using the method proposed in this study, the total time will be reduced to

$$T_{\text{total-manifest}} = \sum_{n=1}^N T_n + T_M + S_1 + T_r + T_{MD} \quad (6)$$

T_M and T_{MD} are the times for hashing metadata and manifest, respectively. The number of calculations needed for verification process is also reduced from $3N$ to $N+4$.

RESULTS

We demonstrated an example of a radiology report containing viewing settings, textual reports, image references, and annotations to be signed using the manifest signature. The radiology report containing several files to present the results of visualization on a web browser is shown in Figure 4. We reconstructed $\text{Ref}(D_n)$ for each file, and created manifest M_D presented as the XML format, as shown in Figure 5. The O_{RG} included four items to identify the clinical documents: discharge note, diagnostic image report, image result, and DICOMDIR. Each item had a resource list to identify the URIs and hash values of

resource data in the item. The clinical data were the Admission.htm, CDA_Report.xml, serimg00001L.jpg, and serimg00002L.jpg, which were converted from the original DICOM file. The CDA_Report.xml was modified from the IHE Simple Image and Numeric Report (SINR). The presentation states were Manifest.xml, CDA_Report.xml, CreateSilverlight.js, and Silverlight.js; the annotations were presented by Ann.xml, which was created from Microsoft Silverlight component. The study images were stored as DICOMDIR.

Performance Analysis

We used the Taiwan Health Professional Card (HPC) with a smart card-based certificate to deal with the cryptography. The average time of one RSA encryption process for 128- or 160-bit digest was about 1.3 s. A Windows PC with Pentium 4 2.0 GHz and 1 GB memory was chosen for demonstrating the results. Figure 6 illustrates the calculation time dependence on the size of the file by using two methods: RSA-MD5 and RSA-SHA1. Figure 7 shows a comparison of the operation time for testing files by one-by-one method (multiple digital signatures) and the manifest method. From the figure, we can find that the time for digital signing was a nearly linear dependence on the number of the files. The differences in calculation time by using the manifest method in three different file sizes (515 KB, 10 MB, and 20 MB) are not obviously different. In the experimental results, the number of files was the most important factor to determine the performance, not file size. Due to the number of RSA encryption process reduced from N to 1,

Fig 6. Performance of signing computation.

Fig 7. Performance of digital signing using one-by-one and manifest methods with different file sizes.

the time needed for the manifest method was much lower than that of one-by-one method.

The Health Certificate Authority Timestamping Authority (HCA-TSA) provides the timestamp service as the TTP. We retrieved the digital time signature from the Health Information Network through the Taiwan Academic Network. Figure 8 illustrates the time distribution of retrieving the digital time signature from HCA-TSA continuously during 1 month period.

An Example of Inconsistent Presentation

In Figures 4 and 5, the CDA_Report.xml was signed as required and the transformation of

presentation was defined in the CDA_Report.xsl. This example illustrates how modifying the presentation data could change the meaning of a clinical document. For example, the gender information (male) in CDA_Report.xml is

```
<administrativeGenderCode codeSystem=
  "2.16.840.1.113883.5.1"code="M"/>
```

The XSLT transformation expressions in CDA_Report.xsl

```
<xsl:variable name="sex" select="administrati-
  veGenderCode/@code"/>
<xsl:when test="$sex='M'"> Male </xsl:when>
<xsl:when test="$sex='F'"> Female </xsl:
  when>
```

transform the value "M" or "F" to "Male" or "Female", respectively. If "Female" and "Male" were interchanged in the above expressions, the patient's sex is changed to female and that is not the correct result, although the original CDA document is not changed.

DISCUSSION

Further characteristics of many EHR formats is the ability to include various components to reconstruct dynamic content in display. Inconsis-

Fig 8. The time distribution of retrieving digital time signature from HCA-TSA. The total retrieval numbers were 3,272, including 17 errors due to the failure of connection. The average time was 1.40 s.

tent presentation of EHR between author and reader is normally caused by the transformation processes. One explanation for this is that the transformation processes were not protected. The transformation processes of EHR obviously should be protected as well as the clinical data if all of these data are protected well under a trusted infrastructure (i.e., PKI). This concept is described in W3C XML Signature as follows:

This recommendation applies to transforms specified within the signature as well as those included as part of the document itself.

In general, most of the medical information standards and national regulations regulating the legal EHR do not consider the presentation problem. The signing range should contain all of the data related to clinical data. If only clinical data is signed and not presentation data, the inconsistent presentation of EHR could happen when presentation data is being modified. There is also some potential risk that the application may be threatened by certain attacks (e.g., phishing, viruses, and Trojan horses). If following different digital signature specifications in the health care domain, the practice will cause lots of trouble. Therefore, a unique signature standard for handling all the clinical data is required.

DICOM suggested composing radiology reports directly in clinical document architecture (CDA) format. DICOM has addressed the digital signature issue of Structure Report (SR), which collects references to a set of related objects into a key object (KO) with digital signatures (i.e., signed KO document). The signed KO document refers to the set of DICOM data objects by using the signed manifest, which means a signed list of multiple digital signatures. It needs many files to construct the presentation of a radiology report. It also requires multiple signatures to secure multiple data format and standards. The performance problem is still not solved in this architecture. If following the existing standards such as DICOM and HL7 to sign radiology report with many files, a great number of digital signatures and digital time signatures are required. It is impractical due to the high computational time of the signing and verifying processes in real-world clinical operations. Fast and reliable proof of authenticity and integrity is needed for security considerations when implementing the digital signature. The manifest signature architecture needs only one

signature to represent the signature for an entire clinical document with multiple data, which can reduce the computation time during signing and verifying processes.

CONCLUSION

Digital signature can provide the authenticity and integrity for digital data, since cryptographic techniques can be algorithmically proven in the radiology field. However, there are many weak points in the processes of digitally signing and verifying data, like the presentation problem and performance issues. How to integrate the multiple data formats and standards becomes an important issue. The manifest signature can provide the framework for handling all clinical data and specifications to realize the security requirements under a trusted relationship. It also can be extended to add the digital timestamp and digital time signature for long-term verifiability. We also addressed the issue of performance during digital signing and verifying. The computational time of the manifest signature is much lower than that of the traditional digital signature method. Following the existing medical information digital signature rules in DICOM, the practice is not feasible. Using the proposed method, the computational time is reduced.

ACKNOWLEDGEMENT

This work was supported by a grant from the National Science Council, Taiwan (NSC 95-2221-E010-003).

REFERENCES

1. The Internet Engineering Task Force (IETF) and World Wide Web Consortium (W3C) XML Signature Working Group, Available at <http://www.w3.org/Signature/>. Accessed 12 June 2008
2. Lekkas D, Gritzalis D: Long-term verifiability of the electronic healthcare records' authenticity. *Int J Med Inform* 76:442–448, 2007
3. van der Haak M, Wolff AC, Brandner R, Drings P, Wannenmacher M, Wetter T: Data security and protection in cross-institutional electronic patient records. *Int J Med Inform* 70:117–130, 2003
4. Schütze B, Kroll M, Geisbe T, Filler TJ: Patient data security in the DICOM standard. *Eur J Radiol* 51:286–289, 2004

5. IHE IT Infrastructure Technical Framework Volume 3 - Document Digital Signature Profile. Available at http://www.ihe.net/Technical_Framework/. Accessed 12 June 2008
6. Health Level 7 (HL7), Clinical Document Architecture, Release 2, Available at <http://www.hl7.org/v3ballot/html/infrastucture/cda/cda.htm>. Accessed 12 June 2008
7. DICOM Supplement 104: DICOM Encapsulation of PDF Documents, Available at ftp://medical.nema.org/medical/dicom/final/sup104_ft.pdf, Accessed 12 June 2008
8. Adobe Developer Resources, Available at http://partners.adobe.com/public/developer/xml/index_arch.html. Accessed 12 June 2008
9. Huang Z, Lu X, Duan H, Li H: Enhanced CDA with electronic signature. The 1st International Conference on Bioinformatics and Biomedical Engineering 1161–1164, 2007
10. Hollerbach A, Brandner R, Bess A, Schmücker P, Bergh B: Electronically signed documents in health care- Analysis and assessment of data formats and transformation. *Methods Inf Med* 44:520–527, 2005
11. Kobayashi LOM, Furuie SS: Proposal for DICOM multiframe medical image integrity and authenticity. *J Digit Imaging* 22:71–83, 2009 doi:10.1007/s10278-008-9103-6
12. Bicakci K, Baykal N: EVEREST: An efficient method for verification of digital signatures in real-time teleradiology. *Stud Health Technol Inform* 107(Pt 2):1241–1245, 2004
13. Rivest RL, Shamir A, Adleman L: A method for obtaining digital signature and public-key cryptosystems. *Commun ACM* 21:120–126, 1978
14. Zhou XQ, Huang HK, Lou SL: Authenticity and integrity of digital mammography images. *IEEE Trans Med Imag* 20:784–791, 2001
15. Zhou Z: Data security assurance in CAD-PACS integration. *Comput Med Imaging Graph* 31:353–360, 2007
16. Kroll M, Schütze B, Geisbe T, Lipinski HG, Gröne-meyer DHW, Filler TJ: Embedded systems for signing medical images using the DICOM standard. *International Congress Series* 1256:849–854, 2003
17. Ruotsalainen P, Manning B: A notary archive model for secure preservation and distribution of electrically signed patient documents. *Int J Med Inform* 76:449–453, 2007
18. World Wide Web Consortium (W3C) XSL Transformations (XSLT), Available at <http://www.w3.org/TR/xslt>. Accessed 12 June 2008
19. World Wide Web Consortium (W3C) XML Signature Requirements, Available at <http://www.w3.org/TR/xmlsig-requirements>. Accessed 12 June 2008
20. Arnellos A, Lekkas D, Spyrou T, Darzentas J: A framework for the analysis of the reliability of digital signatures for secure e-commerce. *The Electronic Journal for E-commerce Tools & Applications (eJETA)* 1(4), 2005
21. Alsaid A, Mitchell CJ: Dynamic content attacks on digital signatures. *Inf Manag Comput Secur* 13:328–336, 2005
22. Jøsang A, AlFayyadh B: Robust WYSIWYS: a method for ensuring that what you see is what you sign. *Proceedings of the Sixth Australasian Conference on Information Security* 81:53–58, 2008
23. Hsiao CH, Hsu TC, Chang J, Yang SJH, Young ST, Chu W: Developing a medical image content repository for E-learning. *J Digit Imaging* 19:207–215, 2006
24. Lien CY, Hsiao CH, Huang LC, Kao T: Authenticity and integrity of portable electronic health records. *Proceedings of International Conference on Health Informatics (HEALTHINF 2008)* 1:67–71, 2008
25. The Sharable Content Object Reference Model (SCORM), 2nd Ed., 2004, Advanced Distributed Learning, Available at <http://www.adlnet.gov>. Accessed 12 June 2008