Journal of Digital Imaging

Security of Patient and Study Data Associated with DICOM Images when Transferred Using Compact Disc Media

Fintan J. McEvoy , and Eiliv Svalastoga

Received: 15 May 2007; Revised: 24 July 2007; Accepted: 5 August 2007

The transmission of patient and imaging data between imaging centers and other interested individuals is increasingly achieved by means of compact disc digital media (CD). These CDs typically contain, in addition to the patient images, a DICOM reader and information about the origin of the data. While equipment manufacturers attach disclaimers to these discs and specify the intended use of such media, they are often the only practical means of transmitting data for small medical, dental, or veterinary medical centers. Images transmitted by these means are used for clinical diagnosis. This has lead to a heavy reliance on the integrity of the data. This report describes attempts to alter significant patient and study data on CD media and their outcome. The results show that data files are extremely vulnerable to alteration, and alterations are not detectable without detailed analysis of file structure. No alterations to the DICOM readers were required to achieve this; changes were applied only to the data files. CDs with altered data can be readily prepared, and from the point of view of individuals viewing the images, function identically to the original manufacturer's CD. Such media should be considered unsafe where there is a potential for financial or other gain to be had from altering the data, and the copy cannot be cross-checked with the original data.

KEY WORDS: Security, telemedicine, medical records

INTRODUCTION

Patient data are often transferred using compact disc media (CD). Manufacturers of digital medical imaging equipment provide the facility to burn a disc containing the patient data in DICOM format together with a DICOM reader. The end user, on inserting such discs into a personal computer (typically running a Windows operating system (Microsoft Corp, USA)) can view the image set. Using an "autorun.exe" file, these discs, once inserted into the CD drive, launch the DICOM viewer and open the patient images or a list of available patient studies.

The security of DICOM files has been discussed in the literature.[1–4] While encryption of patient and study data is possible, it has not been done in many of the software packages on current release. Thus, there is a possibility that significant data such as patient identification number, age, and name can be altered with the result that the reader is mislead. A similar concern exists in the DICOM structured report, which by design, is intended to travel outside the radiology department. A different file standard for example Health Level 7 (HL7) may be used to effect such data transfer, but the encoding process required uses the basic DICOM data as input.

The purpose of this technical note is to explore the ease with which patient and study data can be altered. It has been prompted by questions from the legal representative of a veterinarian's client, who asked in addition to a second opinion on the content of the images, if the patient name, date of the study, and institution where the study was performed can be determined from the images as presented on CD and if so with what certainty.

From the Department of Small Animal Clinical Sciences, Faculty of Life Sciences, Frederiksberg Campus, University of Copenhagen, Copenhagen, Denmark.

Correspondence to: Fintan J. McEvoy; e-mail: fme@life.ku.dk

Online publication 21 August 2007
doi: 10.1007/s10278-007-9068-x

When the question was put and after some review of the literature, it was considered that it would be outside the normal competency of a veterinarian to alter such data and that the data appearing on the screen can be accepted as the data that was originally associated with the image when it was created. This report describes the outcome of an effort to test the security of these data.

MATERIALS AND METHODS

Image CDs produced by the software supplied with computed radiography units from Agfa and Fuji were examined.

The following software was used:

Microsoft Access (a database program), Microsoft Word and Word Pad (Microsoft Corporation , USA).

DicomWorks, (a free DICOM viewer and utility program available at http://dicom.online.fr).

Access PassView v1.12 (a free utility for recovering and displaying Microsoft Access database passwords, available at http://www.nirsoft.net/utils/accesspv.htm).

The content of both CDs was copied onto a partitioned drive of a PC running Windows XP (Microsoft Corp, USA). Folders were created to contain the entire content for each disc. Properties for these folders were then set to "shared" and each was then mapped to a network drive. This step permitted the content of the CD to run directly from the hard drive rather than from the CD. Also, changes could be written to the files and their effects tested using the "autorun.exe" file.

Each CD was viewed in the DICOM reader supplied by the manufacturer and data fields that contain potentially important patient information were identified. For the purposes of this study, fields of interest were patient identification number, name, age, date of birth, study accession number, date of study, and institution.

The viewers were then closed, and the content of the each CD examined using the standard file browser in Windows. The Agfa CD contained data in a Microsoft Access database. The password required to see and alter the file structure was revealed using Access PassView. Images in both CDs were opened and their tags edited using DicomWorks.

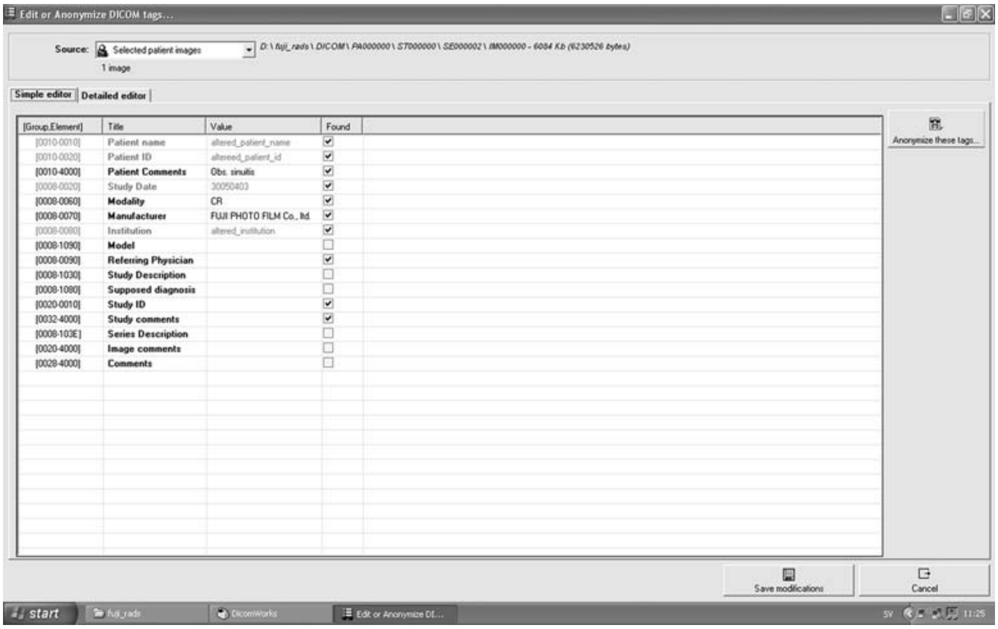
As the aim of the study was to gauge the ease with which credible alteration can be made, a time limit of 2 days per manufacturers' CD was set for the task. No expert computer assistance was used; the authors who are veterinarians specializing in diagnostic imaging have no formal training in computing, but are experienced users of database, DICOM, and "html" files.

RESULTS

Agfa CD The viewer supplied with this CD when launched displays a welcome page. This contains a manufacturer's disclaimer, together with patient and study data. The source of this information is a file titled "about.htm". When this window is closed, the images are displayed. In this display, important patient data is superimposed on the image and is also present within framed fields in the menu bar. Further information is available in a separate window, one for each image, by selecting the "info" icon on the menu bar when the image is open.

All information in the "about.htm" file can be viewed directly and edited in Microsoft Word. Information superimposed on the images in the viewer is taken from the DICOM image file. Opening these ".dcm" files in DicomWorks allows the headers to be viewed and edited (Fig. 1). All text is unencrypted so that it is relatively simple to identify original text that one may wish to alter; in addition, the title of each DICOM tag is shown so tags for placement of patient ID, patient name, and the other information considered important for this study were clearly marked. This DICOM editor indicates which tags are critical to proper functioning of the file. Tags for all information shown in the DICOM viewer were noncritical and could be edited and changes saved.

The information shown in the menu bar on the DICOM reader originates from the Microsoft Access database. While this is protected by password, finding a free program to display the password was not difficult. On looking at CDs generated from a number of Agfa systems, all sold within Scandinavia, it was noticed that the password used was the same. Once opened, the structure of the database was readily examined. There are some 120 tables, but the use of



Edit or Anonymize DICOM tags...

Source: Selected patient images D:\ fuji_rads \ DICOM \ PA000000 \ ST000000 \ SE000002 \ IM000000 - 6084 Kb (6230526 bytes)

1 image

[Group,Element]	Title	Value	Found
[0010-0010]	Patient name	altered_patient_name	☑
[0010-0020]	Patient ID	altereed_patient_id	☑
[0010-4000]	Patient Comments	Obs. sinuitis	☑
[0008-0020]	Study Date	30050403	☑
[0008-0060]	Modality	CR	☑
[0008-0070]	Manufacturer	FUJI PHOTO FILM Co., ltd.	☑
[0008-0080]	Institution	altered_institution	☑
[0008-1090]	Model		□
[0008-0090]	Referring Physician		☑
[0008-1030]	Study Description		□
[0008-1080]	Supposed diagnosis		□
[0020-0010]	Study ID		☑
[0032-4000]	Study comments		☑
[0008-103E]	Series Description		□
[0020-4000]	Image comments		□
[0028-4000]	Comments		□

Fig. 1. Screen capture showing detail of the DICOM tag editor in DicomWorks. Changes to the fields “Patient name”, “Patient ID”, “Study Date” and “institution” have been completed.

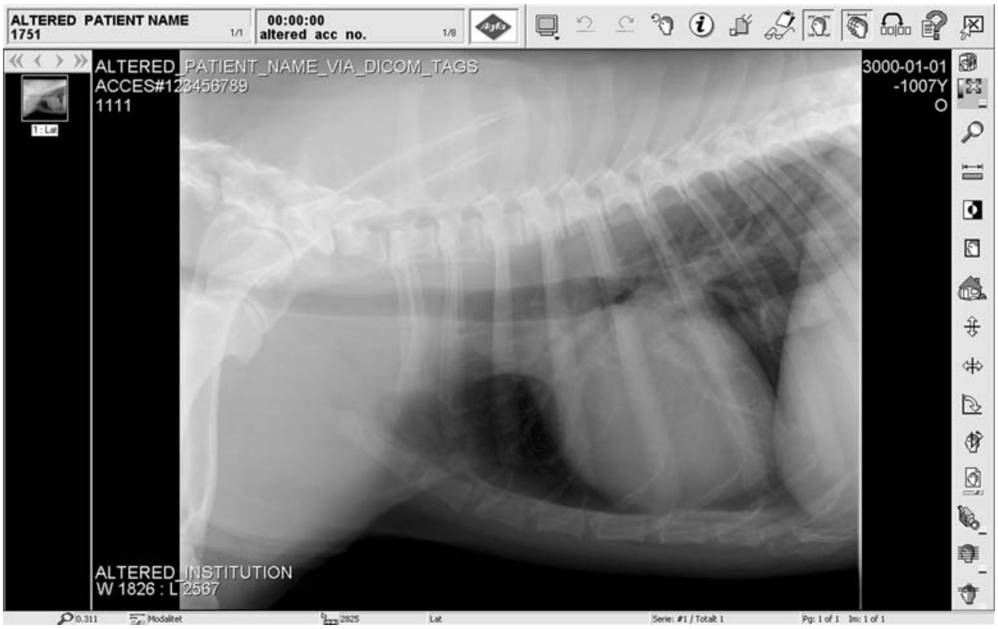
meaningful table names is helpful in navigation. The relevant table was selected and opened. This contained all the study information that was displayed in the viewer. Again, the information is not encrypted, so the existing content of the various tags indicated where alterations are to be made. Changes made could then be saved.

Finally, a new CD was burned containing the altered, “about.htm”, “.dcm” files, and the “.mdb” file (database file). Other files present on the original disc were copied without alteration. The resulting CD ran exactly as the original, except that all the fields selected for change displayed the altered data (Fig. 2).

Fuji CD The Fuji CD uses “eFilm Lite” software. It is opened once the CD containing the data is inserted into a CD drive. On opening, the user is referred to the License agreement. There follows a list of available studies on the CD. Selecting a study from this list opens the images. In the viewer, patient data is superimposed on the medical image. The viewer on this CD uses the “dicom.dir” file and the information contained in the DICOM tags of each image. Simply editing the tags in the DICOM files caused the link between the “dicom.dir” and the images to be lost. As a work around, the individual “.dcm” image files were opened, and their tags edited using DicomWorks as had been done with the Agfa CD. When all the desired changes were made, a new “dicom.dir” file was created using the DicomWorks export facility. This allows the creation DICOM CDs which contain the DICOM images and a freshly built “dicom.dir” file. This latter file can be read by eFilm, so that an altered list of available studies is produced, and selection of a study opens the appropriate, altered, DICOM image file (Fig. 3). Again, a fresh CD containing the altered DICOM image files and the new “dicom.dir” file, together with the original “autorun.exe” and remaining files was burned, and when used, opened in the same way as the original Fuji disc but displayed the altered data.

DISCUSSION

It was assumed that the CD examples used are typical of products on current release. The particular products used were chosen because of availability or are in current use at the authors’



ALTERED PATIENT NAME
1751 1/1

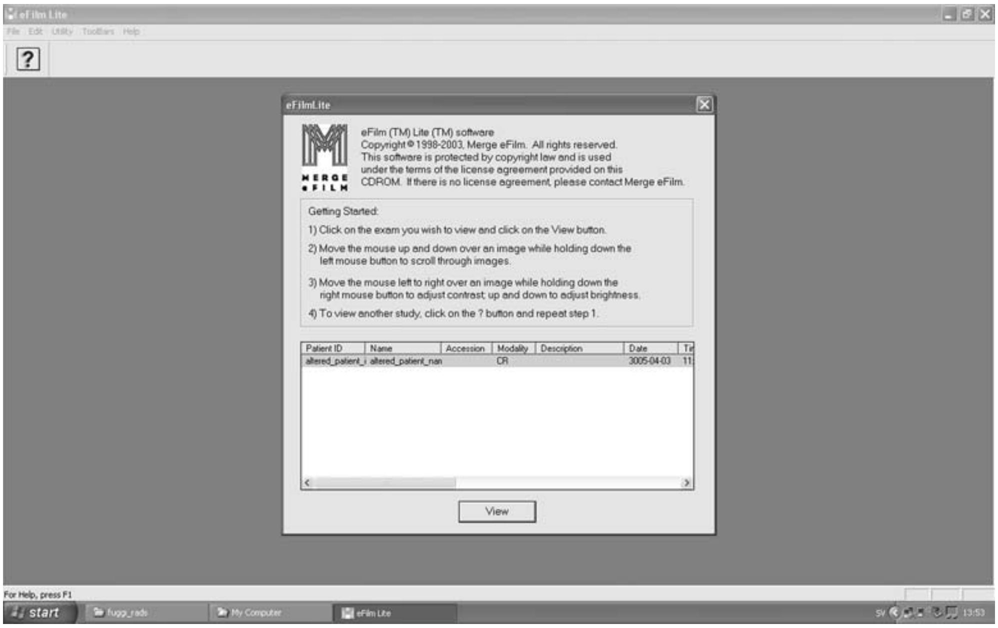
00:00:00
altered acc no. 1/8

ALTERED_PATIENT_NAME_VIA_DICOM_TAGS
ACCES#123456789
1111

3000-01-01
-1007Y
O

ALTERED_INSTITUTION
W 1826 : L 2567

Fig. 2. Screen capture of the image display window provided with the Agfa DICOM viewer. The image shows the thorax of a dog. Altered fields are seen in the upper menu bar and superimposed on the image. The accession number superimposed on the image marked "ACCESS#" differed from the number in the menu bar. The source of the number in each location differs and data at both locations were altered.



eFilm (TM) Lite (TM) software
Copyright © 1998-2003, Merge eFilm. All rights reserved.
This software is protected by copyright law and is used
under the terms of the license agreement provided on this
CDROM. If there is no license agreement, please contact Merge eFilm.

Getting Started:

1) Click on the exam you wish to view and click on the View button.

2) Move the mouse up and down over an image while holding down the left mouse button to scroll through images.

3) Move the mouse left to right over an image while holding down the right mouse button to adjust contrast; up and down to adjust brightness.

4) To view another study, click on the ? button and repeat step 1.

Patient ID	Name	Accession	Modality	Description	Date	Ti
altered_patient_i	altered_patient_nan		CR		3005-04-03	11

Fig. 3. Screen capture from the opening dialog of the eFilm™ Lite™ software used by Fuji. The data in the list field is taken from the altered "dicom.dir" file made by DicomWorks". The user selects the study, and by mouse clicking, opens the (altered) images in the usual fashion.

department. It is accepted that manufacturers may state in an opening window that the discs are for reference and are not to be used for diagnostic purposes. Notwithstanding this, patient information including images, is transferred by means of CD, as in many situations this is the only method of communication for these data.

CDs may be used by design to transfer patient data between clinics and hospitals, a practice which is increasing. This is a positive development in terms of costs but there are associated problems. To include these data in the PACS system of the receiving institute, DICOM data may require alteration (reconciliation) to comply with, for example, local Patient ID and accession number formats. Software to facilitate such reconciliation is commercially available (Dicom Open LiteBox; ETIAM, Rennes, France)[5] and available as open source.[6] It is clear that data transferred by these means are safe insofar as accidental alteration and mismatching of images with patient or study data is concerned, and intentional alterations can be made to the data as part of normal good record keeping. However, this report indicates that if there is a malicious intent, then the data is completely vulnerable and readily altered by individuals with very modest computer skills.

The file modifications described in this report were limited to data files. No alterations to the DICOM readers were made. The data alterations made were sufficient in content and hidden to such a degree that the altered discs could be misleading. This is particularly so if the images are read using the DICOM reader included on the CD. However, a forensic examination of the files would quickly reveal discrepancies in file data and structure. Against that, it is possible that an individual with suitable expertise in computing could effect changes and hide tracks, rendering detection much more difficult. The software used to effect the changes described in this study is widely available. The material used was from computed radiography only. While it is likely that CDs containing DICOM images from direct radiography, computed tomography, magnetic resonance imaging, and ultrasonography are no more robust than the image modality examined here, it would be interesting to extend the study to cover all modalities and a wider range of manufacturers.

In veterinary medicine there can be financial incentives to alter such data. In the horse industry, radiographs are used as part of pre-purchase examinations and for insurance purposes.[7] While the practice of medical imaging is not the authors' area of expertise, incentives undoubtedly exist. The alteration of image data has been highlighted in the field of dentistry, where image alterations can mask or create lesions,[8] which, it is proposed, could be used in the preparation of false insurance claims and to cover traces of unsatisfactory treatments. In addition, it is conceivable that situations might arise where there was a pressure to fraudulently alter a patient's examination date or some other component of study or patient information.

The need for encryption of data in DICOM files is well-recognized.[3] These authors have looked at the practicalities of achieving this and noted that the DICOM standard in requiring patient relevant fields, to be completed often with data in a certain format, can cause difficulties. A common approach to encryption is to replace certain characters according to a key; the resulting special characters may then be unusable in the DICOM file as they do not meet the DICOM standard. A workable approach to this problem has been described.[3] These authors copied data from the DICOM files to a relational database, encrypted it, and then replaced patient data with permissible but meaningless information in the DICOM file. This, to some extent, is the structure of the Agfa CD, except that the database used is not secure; there is no encryption of its content nor is there replacement of data in the DICOM files. Other authors[9] describe security under three logical subheadings, namely, application of a digital signature to the data, so that files can be traced to the unit that produced them and alterations rendered detectable, techniques for secure communication, relating to network security issues and security of the data exchange itself. The last issue related to encryption methods (Basic DICOM Media Security Profiles), which are now part of the DICOM standard. The digital signature on the image itself may be in the form of a digital watermark that is imbedded in the data of the actual image file. These are used for copyright protection where the watermark is said to be robust and for content authentication where the watermark is easily damaged by attempts to alter image content and so is termed fragile.[10] The watermark may be coded and require a digital key to permit decoding. Procedures that insert watermarking data over the entire image or into a polygon selection that is outside the image area that displays the patient are described. Recently, lossless reversible methods to achieve this have been reported.[11,12] This method overcomes the inherent weakness in any strategy that identifies images by data in associated tags. Watermarks can be used to identify the source of an image. This is important for copyright protection. They may also contain information that is unique to the subject of the image, i.e., the patient, and would so provide security against the alterations made in this study. Thus, the content of the watermark would not match the content of the DICOM tags, so data alteration would be suspected. Finally, watermarking procedures should not interfere with interpretation, and this goal appears to be readily achievable.

While it is clear that manufacturers have technology to address security issues, the implementation of these measures is only recent or has yet to happen. Also, when implemented, they may not be applied retrospectively, so that older units will contain serious security vulnerabilities.

Users should be aware of the vulnerability to alteration of study and image data when transmitted via CD media. The need for data that is robust and secure should be communicated to the manufacturers, and professionals involved in imaging should not compromise themselves by using these media for anything other than the usage the manufacturers approve in their license agreements and program documentation.

REFERENCES

1. Engelmann U, Schroeter A, Schwab M, Eisenmann U, Vetter M, Lorenz K, et al: Borderless teleradiology with CHILI. J Med Internet Res 1(2):E8, 1999 Oct–Dec

2. Bernarding J, Thiel A, Decker I, Grzesik A, Wolf KJ, Tolxdorff T: Prototype of a JAVA/DICOM image server with integrated findings and data security. Stud Health Technol Inform 77:865–869, 2000

3. Bernarding J, Thiel A, Grzesik A: A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption. Int J Med Inform 64(2–3):429–438, 2001 Dec

4. Schutze B, Kroll M, Filler TJ: A solution to add digital signatures to medical images according to the DICOM standard: embedded systems. Rofo 177(1):124–129, 2005 Jan

5. van Ooijen PM, Roosjen R, de Blecourt MJ, van Dam R, Broekema A, Oudkerk M: Evaluation of the use of CD-ROM upload into the PACS or institutional web server. J Digit Imaging 19 Suppl 1:72–77, 2006

6. Hacklander T, Martin J, Kleber K: Informatics in radiology (infoRAD): an open source framework for modification and communication of DICOM objects. Radiographics 25 (6):1709–1721, 2005 Nov–Dec

7. McEvoy F, Rossdale PD, Wingfield Digby N, Lane JG: Caveat vendor: technology and prepurchase examinations of horses. Equine Vet J 30(4):274–276, 1998 Jul

8. Guneri P, Akdeniz BG: Fraudulent management of digital endodontic images. Int Endod J 37(3):214–220, 2004 Mar

9. Schutze B, Kroll M, Geisbe T, Filler TJ: Patient data security in the DICOM standard. Eur J Radiol 51(3):286–289, 2004 Sep

10. Queluz MP: Authentication of digital images and video: Generic models and a new contribution. Signal Processing: Image Communication 16(5):461–475, 2001/1

11. Alattar AM: Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156, 2004 Aug

12. Guo X, Zhuang TG: A Region-Based Lossless Watermarking Scheme for Enhancing Security of Medical Data. J Digit Imaging 2007 Jul 10 DOI 10.1007/s10278-007-9043-6