Photographic Images, Digital Imaging, Dermatology, and the Law

Noah Scheinfeld, MD, JD

**Background:** Patient photographic images play an important role in dermatological record keeping and training. An assessment of the legal implications of image taking is necessary to use images properly.

**Observations:** Images are parts of the medical record and must be treated with the same care as written medical records. Because multiple digital images are sometimes taken and digital images can be easily manipulated, they present novel issues in this regard. Images can be used as evidence in court. Issues regarding digital images include (1) authentication, (2) manipulation, (3) audit trail verification, and (4) data compression. The Health Information Portability and Accountability Act requires that health care providers control and track those who have access to identifiable digital medical information. This should facilitate the use of digital images as evidence because the provenance of digital images can be established. The Health Information Portability and Accountability Act covers the use and disclosure of protected health information, such as “full-face photographic images and any comparable images.” To publish identifiable digital images (images of the face), it seems prudent for patients to waive in writing their rights to this protected health information.

**Conclusion:** Images will continue to enhance dermatological care, and understanding and accounting for the legal underpinnings of their use is prudent.

Arch Dermatol. 2004;140:473-476

---

**Observation**

**Images and Medical Records**

All physical information that a physician assembles while providing medical care is part of the medical record. In the United States, states have legislation that requires that medical records cannot be tampered with or altered and explicitly defines the duration for which records must be kept, and such legislation frequently imposes criminal or civil penalties for the alteration or destruction of medical records. The federal government has similar requirements and requires that medical records be maintained for 5 years and contain the “results of all consultative evaluations of the patient as well as appropriate certain findings by clinical and other staff involved in the care of the patient.” Some state courts deem that the destruction of medical records can be adduced as proof that a physician committed malpractice. In one federal case in Arkansas, a court, in its orders to the jury, stated that a medical record that was destroyed by workers in an emergency room could establish a defendant physician’s liability for negligence. Therefore, physicians must heed medical record maintenance requirements.

In view of the foregoing, images that are captured to document the appear-
ance of a patient as part of his or her medical care are clearly parts of such a patient’s medical records. The combination of written text medical records and film photographs can be achieved by stapling the photographs into the medical chart. It is more difficult to combine digital images with written charts. Leaving images on a computer hard drive or CD-ROM not attached to the medical chart results in chart data being in 2 places (ie, parallel charts), complicating access, storage, and efforts at audits of medical records containing such images. This same problem exists with electronic medical records that cannot accommodate images. This could also be an issue with teledermatology records in which images were not parts of the teledermatology medical record itself. Although no case law has been found on this issue, it seems prudent to attach all pictures (in their original form) taken of a patient during evaluation and treatment, rather than have 2 parallel records, one written and the other photographic, in different locations.

Patient photographic images not captured for medical care present other legal issues. If images are acquired by a treating physician for reasons other than medical documentation (ie, publication, recording for a medical conference, or a clinical trial), it is unclear if such images might be deemed to be part of the medical record. The expectation of the patient as to whether such images would be kept with his or her medical records might shape a court’s classification of such images. A court probably would not view images captured by someone who was not a patient’s physician or associated with this physician as parts of such a patient’s medical records.

**DIGITAL IMAGES AS MEDICAL RECORDS**

Digital images can be useful in providing dermatological care, particularly in teledermatology systems deployed in remote or underserved areas. Their use has not been tested in much litigation. A 1997 article noted that no cases involving digital images had been reported in the previous 10 years. Since that time, several courts have assessed the use of digital images. Federal courts have ruled that digital images can furnish sufficient medical data to provide dermatological care. Digital images may present challenges to physicians who are new users of this technology as to what is to be included in the medical record. Is the digital image or a print of the digital image considered to be the original from a medical and evidentiary standpoint? The House of Lords fifth report on Science and Technology, quoted by Barry et al, noted that paper copies of digital images are rarely needed for patient care and that digital images benefit legally from authentication techniques:

> We find that there is some confusion over what can be described as the original when considering the digital image, in particular between the technical and legal definition. We prefer the following definition in relation to digital images: the original is the data first recorded in memory. Thus any printed or displayed image created from these data is a copy. Consequently, digital record recording technology provides no original that could be produced in evidence. All that is available for use as evidence is a copy of the first, probably temporary, recording in memory, and this will be admissible as evidence. Its weight as evidence will depend on proper authentication and other matters.

It is unclear if all images captured of a patient at a visit are parts of the medical record. Often, multiple digital images are taken and some immediately erased because they are not useful, clear, or appropriate. Although it would seem that these images are not part of the medical record, a patient could claim that these images were in fact representative of the skin condition. Conflicting analogies for this situation exist. Inadequate or contaminated blood samples are sometimes not sent to the laboratory and at other times are sent and then noted in the laboratory as contaminated (hemolyzed) and a new sample requested (although all records are kept). Is a poor-quality image to be discarded or saved and not used? It would seem best to save it and not use it to protect the physician from claims of discarding medical data. Similarly, when digital manipulation enhances the digital images for clinical interpretation, it is suggested that the manipulated and original images be archived to avoid debate on the extent to which an image has been altered.

Case law exists that only saving the single best image or having definitive proof images were not altered will not lead to an inference that the defendant destroyed or altered evidence. In *Scardina vs Maersk Line, Ltd.*, a slip-and-fall case on a ship, the plaintiff complained specifically that the defendant failed or refused to produce all original photographs and digital photographs taken of his back during his physical examination on the vessel after his fall. The defendant claimed that the one photograph of his back produced and admitted into evidence could have been altered by the defendant, and that the photograph was not authenticated. The court stated that the jury could reasonably have concluded that the defendant reviewed the photographs and simply selected the clearest one to keep, then discarded any others along with the digital file. Absent any evidence to the contrary, the court explained the plaintiff was not entitled to an “adverse inference” jury instruction on the issue.

**PHOTOGRAPHIC IMAGES AS EVIDENCE**

Images can be used as evidence in court. Since the 1860s, courts have used photographs and photographic enlargements. Photographs must be authenticated in a fashion similar to other evidence. To admit an image into evidence, a litigant must lay a legal foundation for it. The image must be shown to be unaltered material with an identifiable chain of custody. It must affect the existence and probative value of factual legal questions. Photographs are important pieces of evidence because psychological tests show that after 3 days a person of average intelligence will remember 65% of what he or she has seen and heard, as opposed to 10% of what was heard without visual evidence.

**SPECIAL CONSIDERATIONS OF DIGITAL IMAGES AS EVIDENCE**

In the United States, current thinking is that digital images are bound by the same legal requirements for chain
of custody and originality that film-based photography and physical evidence are. Several aspects of digital images, however, suggest that their legal treatment might differ from that of film images when they are used as evidence. These aspects are (1) authentication of such images, (2) ease of manipulation of digital images, (3) need for an audit trail because of the ease of manipulation of the images, and (4) compression of data that occurs in many cases when digital images are stored. The successful introduction of digital images as forensic evidence in a court of law is dependent on its reliability, reproducibility, security, and usefulness in the discovery accompanying litigation and in the courtroom.10-13

Proving that a digital image has not been altered and is authentic presents challenges. Digital images can be manipulated easily.14 Legal analysts of dental radiography have noted that digital dental images (including hard-drive records) may also be altered easily15 and that altered images have been used to commit fraud.16 These manipulations include changing the contrast, colors, and object borders of images. Therefore, in the British Government’s response to the House of Lords guidelines on digital images as evidence, suggestion that legal bodies draw greater attention to the digital processing and to widen public awareness that paper originals are rarely necessary, it stated that “the Government agrees with this proposal but notes that while paper originals may rarely be necessary, retention of the original digital file, captured from the original paper or other source, is considered highly desirable, if not essential.”17 Courts must use their standard procedures (examining witness and physical evidence) to authenticate digital images.

Altering an image (eg, sharpening the borders of objects in an image) sometimes enhances its usefulness. Sharpening procedures must be reproducible so that courts can evaluate such procedures when evaluating images as evidence.

The HIPAA requires that all identifiable digital medical information be kept private and secure. The HIPAA mandates that health care providers control and track those who have access to identifiable digital medical information. This should facilitate the use of digital images as evidence because the provenance of digital images will be established, ie, we will know who looked at images, when and where this occurred, and what they did with them. Under the HIPAA, questions regarding the provenance of digital images are addressed to an extent not seen before, potentially rendering them usable evidence for the information that they captured. Unaltered digital images can be provided to plaintiffs in litigation during discovery, facilitating the admission into evidence of images in litigation.

Digital images do not always capture all the extant image data. Digital cameras capture data (pixels, or picture elements) and then store them. Images can be saved as (compressed or lossy) Joint Photographic Experts Group (JPEG) files or as uncompressed tag image file format (TIFF) files. A JPEG is an algorithm whereby similar pixels are stored as identical pixels, thereby decreasing the amount of data to be stored, resulting in the loss of some data. Use of JPEG images saves memory space and makes images easier to store and manipulate. A 3-megapixel camera can store an image as a high-quality JPEG image in a 1-megabyte file or in TIFF as a 10-megabyte file. Investigations in radiology have shown that JPEGs compressed 1:15 relative to TIFF images do not lead to any change in clinically relevant data.18 As computers increase in speed and as storage costs fall and improved nonlossy algorithms become more widely accepted, it seems optimal that digital images for medical records be stored in nonlossy formats.19 No law exists on whether TIFF images should be saved rather than JPEG images. However, because JPEG images are generally sufficient to make clinical diagnoses, they should be evidence of sufficient quality to adduce in court.

**PENALTIES FOR IMAGES MISUSE**

A special legal relationship exists between patients and their physicians. It is a fiduciary relationship. The information provided by a patient to physicians is confidential in part because of this fiduciary relationship. Although the law recognizes that information needs to be transmitted to other physicians to provide treatment to patients, these other physicians are then bound to treat the information as confidential. The medical record and the images of the patient therein must be kept private. A person divulging patient information in circumstances that do not maintain patients’ privacy can be sued by affected patients to stop the information from being divulged and can seek damages for any loss suffered from the breach. The ease with which digital images may be transmitted and replicated might evoke special vigilance on the part of physicians to keep them private and confidential.

**HIPAA AND THE PRIVACY OF MEDICAL IMAGES**

The HIPAA adds special strictures to the use of digital images and imposes penalties for the violation of its provisions. The HIPAA applies to identifiable medical information and does not apply to film photographs. The content of the HIPAA has been outlined elsewhere, so this article focuses on its relationship with digital images. The HIPAA Privacy Rule covers the use and disclosure of protected health information, such as “full-face photographic images and any comparable images.”20 In specific instances, patients can waive in writing their rights under the HIPAA. I suggest that the consent should note that the patient authorizes a practice or physician to make use and disclosure of protected private information about a patient in the medical records as it pertains to a patient’s identifiable images. The consent would also state what publication would publish these images. A precise description of the images and the purpose for publication would be included in the consent. The consent would also have the patient’s name, address, medical record number (if applicable), and Social Security number. A complicating factor in this is that the HIPAA allows patients to revoke consent for disclosure at any time. How this would be affected after facial images have already been published has yet to be defined, but it should not effect a published work because such images are parts of a scholarly work rather than the medical record.
CONCLUSIONS

Images are an important part of the medical record. They can be used as evidence in court. Digital images can be used by physicians in medical care and function as parts of the medical record if attention is paid to ensure their reliability, reproducibility, security, and usefulness in discovery and litigation. The HIPAA will make it easier to use digital images as evidence because it controls who sees them and what is done with them. It is optimal to maintain all medical images and to acquire the highest quality (i.e., uncompressed) images possible. Digital images engender several novel legal issues, but these can be dealt with in ways that optimize medical care and legal compliance.

Accepted for publication October 10, 2003.
Corresponding author: Noah Scheinfeld, MD, JD, Department of Dermatology, St Luke's–Roosevelt Hospital Center, 1090 Amsterdam Ave, Suite 11D, New York, NY 10025 (e-mail: Scheinfeld@RCN.com).

REFERENCES