Chapter 34
Medical Records: Paper and Electronic

S. SANDY SANBAR, MD, PhD, JD, FCLM

The purpose of the medical record is to document comprehensively pertinent medical or health information about patients, including diagnosis and treatment of diseases, victims of domestic violence, victims of elder and child abuse, workplace accident victims, injuries of crime victims, and personal injury litigants. In addition the medical record may play a vital role in courtroom competency issues in a variety of estate, criminal, and civil commitment cases.

Medical records are currently being radically transformed in what is best described as an era of transition. The traditional paper medical records, whether handwritten or typed, are becoming electronically supplemented or replaced, in part or in whole, by hard drives and backup tapes, CDs and DVDs. The health care industry is rapidly and increasingly becoming computerized in the United States. In contrast to its paper counterpart, the electronic medical record is an electronically stored database containing a patient's health care information from one or multiple sources, including imaging of paper records.

ADVANTAGES AND DISADVANTAGES OF ELECTRONIC MEDICAL RECORDS

From a medical standpoint, electronic medical records have certain advantages over paper records. They require less storage space, and they can be stored indefinitely. They facilitate effective quality assurance, analysis of practice patterns, and research activities; speed the retrieval of data and expedite billing;[1] reduce the number of lost records; allow for a complete set of backup records at little or no cost; expedite the transfer of data between facilities, regardless of geographic separation; are a proven long-term cost reducer; and, in most cases, are practice enhancers and a public relations tool. In some hospitals and clinics they have reduced the number of transcriptionists needed. The introduction of wireless and hand-held devices has greatly increased the versatility of electronic record entry and retrieval. Advances in natural language processing software have made screening free text records faster and more accurate than previously thought possible, and the field continues to develop.[2]

From a legal standpoint, first and foremost, an electronic record system will produce a legible record.[3] Many of the problems of wrong medication, wrong dose, wrong directions, wrong procedure caused by illegible and misinterpreted records will be eliminated. Second, a properly planned medical record system can incorporate practice guidelines that are automatically triggered by a diagnosis or symptom syndrome.[4] Adherence to practice guidelines has been an effective defense in many malpractice actions. Guidelines have also been championed as the most effective method of eliminating unnecessary and costly defensive medicine practices.[5] In a like manner, the effective electronic medical record system will have connections to the pharmacy and pharmacy data banks. Computerized prescriptions and orders will not permit prescriptions or orders for drugs for which the patient has a known allergy, and the system will alert both provider and pharmacist of potentially harmful drug–drug interactions or incompatibilities with the patient's physical or laboratory findings.[6] Adverse drug events are now the number one adverse hospital event[7] and second only to birth injuries in the amount of damages paid in malpractice claims. Reducing these adverse events would be an important risk management accomplishment. Fourth, electronic medical record systems can track ordered laboratory, diagnostic, or imaging tests, alert the provider of abnormal tests, and even notify the patient of the need, or the lack thereof, of future tests, diagnosis, or treatment.[8] Fifth, electronic medical records automatically confirm the date and times of all entries and keep a dated and timed log of all individuals who have accessed the record. Many individuals think these features make electronic medical records more secure than paper records. In any case, such entries offer great protection against accusations of Medicare or Medicaid fraud and abuse. Sixth, most electronic record systems automatically generate patient educational materials tailored to the patient's diagnosis and treatment. These defensive features are hard to beat in a paper system. Seventh, in professional liability suits against health care providers the medical record is "The witness that never dies." A well-documented, complete, and unambiguous medical record means a case that is infinitely easier to defend.

Electronic records have some well-known problems. Critics cite high initial cost, large training investment, hardware crashes and breakdowns, power failures, software glitches, sabotage of the system by disgruntled employees and hackers, unauthorized access, viruses, Trojan horses, reluctance of physicians to use the tightly controlled format for notes, and a host of other real and imagined problems.[9]

STANDARDS OF RECORD-KEEPING

Three overlapping bodies or regulations determine the standards for medical record-keeping: (1) individual state statutes or administrative regulations; (2) specific health regulations and/or regulations for business records, which detail what should be entered and contained, the mechanics of entry, and the authentication of the records;[10] and (3) local regulations. All three of the regulating bodies tend to treat medical records seamlessly from the outpatient setting to the extended care facility.

The next layer of control is exerted by JCAHO. JCAHO has extremely extensive and detailed standards for medical records located in two sections of their accreditation manual, *Assessment of Patients and Information Management Planning*.[11] However, the detail in the JCAHO's standards is more concerned with the content and handling of the medical records entry than with the mechanics of entry. The JCAHO standards also attempt to incorporate the third layer of control, the federal regulations, including those of Medicare.[12]

Hospital staffs, managed care organizations, and clinics may assert institutional requirements applicable to their records that exceed or are in addition to the above layers of control.

Medical Record Entries

Most jurisdictions require that the record be written in ink and be in English. However, electronic medical records are increasingly being accepted and legalized. The entries should be direct, concise, clear, complete, and unambiguous. Medical record entries are to be made contemporaneously with the event. The entries are not to be postponed to a more convenient time or to the end of the day. They are to be written or dictated contemporaneously with the care and/or treatment, producing a record in chronological order. There is no justifiable reason for the record not to be in chronological order. Medical record entries should aim at conveying all relevant, objective, accurate information concerning the patient into the record. Subjective conjecture or opinion information should not be entered. Abbreviations and acronyms should be routinely avoided to eliminate the possibility of confusion. Entries must be legible if entered by hand and, in most jurisdictions, may be entered by typewriter or computer to ensure legibility. *No entry in the medical record should ever be altered or backdated!* All entries should be signed or otherwise authenticated in a legal manner and timed and dated.

Electronic Record Criteria

As with paper records, properly compiled and maintained electronic medical records are business records.[13] As such they must meet certain criteria to ensure their admissibility as evidence in court. The most critical element in the admissibility of electronic records is reliability. When a paper record is prepared, it is fixed in form and content. In most cases changes may be detected. The electronic media may be changed and the changed product may be indistinguishable from the original. Therefore, the first criterion to be met is that the electronic medical record must place each entry as made in a "read only" mode. That is, once the entry is made, it cannot be altered. Any changes must be made by a new note entered in order, dated, and timed.

Although no formal criteria have yet been published, the following criteria must be adhered to for electronic data to be considered "records" in the evidentiary sense:

- *Compliant*. Information-keeping must adhere to local jurisdictional requirements for admissibility as "business records."
- *Responsible*. Written policies and procedures for record storage and maintenance must be established and maintained.
- *Implemented*. The written policies and procedures must be employed at all times.
- *Consistent*. Record-maintenance systems must ensure that records stored and maintained are managed in a uniform fashion to ensure credibility.
- *Comprehensive*. All business records must be stored and maintained.
- *Identifiable*. All business records for a discrete transaction must be readily identifiable and accessible.
- *Complete*. Stored records must preserve the content and structure of the business transaction creating them to ensure accuracy and understanding.
- *Authorized*. All maintained records must have been stored under the auspices of an authorized creator.
- *Preserved*. Records must be inviolate to preserve their original content. No records may be audited without a concise audit trail that preserves relevant information of the original content.
- *Removable*. Records may be removed from storage only with the consent of an authorized entity. All removals must be evidenced by an audit trail that preserves the content of the record being removed.
- *Usable*. The information in the stored records must be accessible for general business purposes, for exportation to reporting functions, and for redaction when necessary. Any and all accesses (even simple reading) must create an audit trail.[14]

A careful analysis of these requirements will stress that, in addition to reliability, generally requiring some sort of emergency power source, both a functioning archival system and a secondary, preferably off the premises, backup system are essential to a well-functioning medical records system. Unfortunately, the backup system, one of the electronic medical record's greatest advantages over the paper system, is the most commonly overlooked element of electronic medical records.

The Federal Rules of Evidence have long recognized the admissibility of electronic business records.[15] In addition, the Federal Rules of Evidence recognize a computer printout as an "original" for the purposes of admission.[16] Most state courts have followed the federal leads on both issues.[17]

Content of the Medical Record

The minimal requirements of JCAHO and Medicare Medicaid for the contents of medical records include the following: identification and demographic information; evidence of informed consent; evidence of known advance directives; admitting complaint or diagnosis; history of the present illness; past history (including social history); family history; orders; laboratory reports; imaging reports; consultations; reports of procedures or tests; progress notes that include clinical observations, results of treatment, and complications; final diagnosis; and discharge summary.

In addition, other items may be required by local statutes or regulations, or a hospital, institution, or specialty organization's specific requirements. The risk manager might also add the following requirements: (1) notations concerning lack of patient cooperation, failure to follow advice, or failure to keep appointments, as well as records of follow-up telephone calls and letters; (2) for any laboratory, radiographic, diagnostic test or consult ordered, the dates ordered, received, and reviewed; and (3) copies of records, instructions, diets, or directions given to the patient or the patient's representative.

Additions, Corrections, Patient Access, and Statements of Disagreement

Corrections and/or additions should be made as outlined in the Uniform Health Care Information Act (UHCIA).[18] The procedure described in the act is quite simple. The health care provider should never expunge or obliterate any material. Instead, the provider should add the correction or addition to the medical record as a new chronological entry. The provider should also mark the corrected or amended record, in its margin, as corrected or amended and indicate where the correction or amendment may be found.[19]

Both the UHCIA and the DHHS regulations, generated in response to the Health Insurance Portability and Accountability Act (HIPAA) (see Chapter 16), provide for patient access in all but a few circumstances.[20] In addition, over 30 states have statutes allowing patients some access to medical records.[21] Both HIPAA and UHCIA allow patients to copy those records and to seek correction of errors within the record.[22] If the provider agrees with the proposed correction or amendment, the provider corrects or amends the record as described above. If the provider disagrees with the proposed correction or amendment, the provider must notify the patient of his or her refusal to correct or amend the record and offer the patient the opportunity to add a concise Statement of Disagreement. On receipt of the Statement of Disagreement, the provider enters it in the medical record, marks the disputed entry as disputed, and identifies where the Statement of Disagreement is located. The UHCIA provides for both civil and criminal penalties if the provider denies patients this right.[23] At least one state court has levied sanctions against a provider who failed to allow a patient legitimate access to his or her medical records.[24]

Alteration, Destruction, or Loss of Medical Records

As noted above, *no entry in the medical record should ever be altered or backdated*. In the law of evidence, the loss, destruction, or significant alteration of evidence is termed "spoliation of evidence." Thus, when medical records that have been altered, or had portions removed, or cases in which the record cannot be found come before the court, the evidentiary concept of spoliation of evidence is invoked. The common law evidentiary inference concept or remedy for spoliation is explained by Wigmore as an indication that the spoiler's case is weak, and "operates, indefinitely though strongly, against *the whole mass of alleged facts constituting his cause*" (2 Wigmore (3d ed. 1940) §278 p. 120 (emphasis added).[25]

Therefore, alterations to records can prove to be disastrous. Records with alterations are absolutely deadly in court. Document examination is now a sophisticated science. With skill and uncanny accuracy, experts may be able to determine the time that entries were made in medical records and who made them.[26]

Courts reason that destroying or altering records in anticipation of or in response to a discovery request falls under the umbrella of misuse of discovery. Discovery rules provide a broad range of sanctions for the misuse of discovery. Sanctions can include monetary fines, contempt charges, establishing or precluding the facts at issue, striking pleadings, dismissing all or parts of the action, and even granting a default judgment against the offending party. In addition to these evidence and discovery sanctions, many penal codes include criminal penalties for perjury and spoliation.[27] In several jurisdictions, spoliation of evidence itself is a cause of action in tort.[28]

Therefore, tampering with medical records may make malpractice cases impossible to defend. Further, providers who falsify a patient's record may be found civilly and criminally liable. Proof of such charges will result in loss of hospital privileges and even loss of license to practice.[29]

Retention of Medical Records

The increased complexity of health care delivery has heightened the importance of medical record retention. It is imperative, apart from any statutory mandates, that a physician maintain comprehensive patient records as long as the threat of a medical malpractice suit exists. That means that, if at all possible, medical records should be maintained indefinitely. A general guideline is to maintain medical records for at least 10 years after the *last* time the patient consulted the health care provider. In the case of minors, the medical records should be kept for a minimum of 10 years or until the patient reaches the age of majority plus the applicable statute of limitations, whichever offers the longer period of time. The presence of a latent injury may extend the statute of limitations until the injury is discovered. Discovery rules in some states will extend malpractice liability beyond the statute of limitations. These rules will usually allow a period of time, most often

1 year, after discovery of the malpractice to bring a suit. In states with such discovery rules, minors' records should be retained for sufficient time for the minor to reach majority and for the statute of repose, if there is one, to expire.[30] If there is no statute of repose, minors' records, and adult records as well, must be kept indefinitely because there is no time limit to bringing a suit under the discovery rule.

If it is impossible for a health care provider to retain the paper medical records indefinitely, records may be stored at a commercial facility, imaged or microfilmed.[31] However, these alternatives are expensive, especially for the physician leaving practice. Many times local clinical or hospitals will agree to maintain the records of a physician retiring or leaving the community in order to establish at least a marginal contact with the physician's former patients. Either as partial consideration in a sale of medical records or as total consideration for the unremunerated transfer of records, a binding written agreement should be made. The agreement should specify the following at a minimum:

- that the transferee will act as trustee of the records for the transferor;
- that the records must be retained for a specific term of years or indefinitely;
- that the trustee will honor the confidentiality of the patient;
- that the patient's requests for copies of all information will be honored;
- that the original provider, his or her attorney-in-fact, and his or her personal representative will have access to and may copy any record;
- that the records may be microfilmed, scanned, or otherwise reduced or compacted at no expense to the original provider;
- that the agreement is binding on the transferee's successors and assigns.[32]

State Regulations

State law may dictate specific medical record retention requirements. For example, employee health records should be retained according to specific state retention requirements.

Federal Regulations

Federal regulations governing the Medicare program require participating hospitals to keep patient records and records of building materials; cost report materials; and reviews, reports, and other records[33] for at least 5 years after a Medicare cost report is filed with the fiscal intermediary or that period of time determined by the appropriate state regulation governing the retention of records, whichever is longer.[34] All records pertaining to any reimbursement issue that is on appeal with the Medicare program should be retained until the conclusion of the appeal.[35]

Methadone treatment programs must maintain records traceable to specific patients, showing dates, quantities, and batch or code marks of the drug dispensed for a period of 3 years after the date of dispensing.[36] Likewise, when narcotic drugs are administered for treatment of narcotic-dependent, hospitalized patients, the hospital must maintain accurate records, showing dates, quantities, and batch or code marks for the drug administered for at least 3 years.[37]

The federal Occupational Safety and Health Administration (OSHA) requires that a provider maintain, for 5 years after the end of the year to which it relates, documentation, consisting of a log and descriptive summary; a supplementary record detailing the injuries and illnesses; and an annual summary, which is to be posted, of an employee's occupational injuries and illnesses.[38]

Other Regulations, Recommendations, and Requirements

JCAHO provides that the length of time for which medical records are to be retained is dependent on the need for their use in continuing patient care, legal research, or educational purposes and on law and regulation.[39] A provider may wish to consider the recommendations of professional associations regarding record retention times. For example, three such associations—the American Hospital Association, the American Medical Association, and the American Medical Record Association—have recommended that the complete patient medical record (in original or reproduced form) be retained for a period of 10 years. This period would commence with the last encounter with a patient. These associations further suggest that after 10 years such records may be destroyed, unless destruction is specifically prohibited by statute, ordinance, regulation, or law, and provided that the institution retains certain information for specified purposes.[40] With respect to electronic medical records, the storage issues have been greatly ameliorated.

Destruction of Medical Records

Some states have specific regulations governing the destruction of medical records.[41] Usually these regulations call for incineration or shredding as a means of protecting patient confidentiality. If a health care entity destroys its own records, it should establish written policies covering the destruction and require a written declaration from the person responsible for record destruction that the prescribed policies were followed. Usually destruction of records will require the use of a commercial document disposal company. It is important that the record destruction by such a commercial entity be covered by a written agreement. That agreement should include provisions that cover the following points:

- the method of destruction;
- warranties that the confidentiality of the records will be honored;
- indemnification for any unauthorized record disclosures;
- a Certificate of Destruction from the commercial entity certifying the date, method, and the complete destruction of the record. The Certificate of Destruction should be retained as a permanent record.

Security and Protection of Medical Records

Although reason would dictate that a certain degree of record security and protection is necessary to prevent unauthorized access to medical records and ensure the integrity of the

information contained therein, there are a few specific guidelines regulating record security and protection.[42] The federal regulations protecting confidentiality of alcohol and drug abuse require that the records be maintained in a secure room, locked file cabinet, safe, or other similar container when not in use.[43] Both the HIPAA Standards for the Privacy of Individually Identifiable Health Information and UHCIA call for providers to effect "reasonable" safeguards for the security of medical records, but do not specify what those reasonable safeguards should be.[44] However, the comments to the UHCIA chapter indicate that the safeguards should be reasonable for the sensitivity of the information contained, the type of provider maintaining the information, and other factors particular to the information's environment. The following are minimal requirements that should be part of any record program:

- a written health care management policy with security and protection provisions;
- a designated individual in charge of record security;
- background checks and bonding of all record personnel;
- training of all medical record personnel in security and privacy issues;
- locked door, authorized entry access to records;
- locked, fireproof record storage;
- locks changed on a regular basis or with a change of personnel;
- passwords, access codes, or advanced recognition technology and firewalls for automated systems;
- confidential material should not be kept on a publicly accessible system and a publicly accessible system should not be run on the institution's internal system;
- passwords and access codes changed on a regular basis;
- written or electronic access and print logs;
- archival and/or backup records stored off-site;
- a zero tolerance for security violations regardless of the form of the records. No record security violation should go unrecorded or unpunished.

Record Retrieval

No record system is complete without an organized method for the retrieval of records. Strange as it may seem, there seem to be few if any regulations governing the retrieval system used, but there are cases reflecting damages for retrieval failures.[45]

OWNERSHIP AND PATIENT ACCESS

There is little controversy about who owns the tangible medical record, that is, the paper, film, or recording that contains the medical information: the health care provider who is responsible for creating, compiling, and maintaining the medical record owns it.[46] In facilities where records are compiled by several individual health care providers, the facility is the owner, not the assorted individual health care providers.[47] The ownership is established by statute in several states and by contract in others.[48] However, the ownership interest in the medical record is different from the ownership interest in most other personal property and is governed by a large body of ethical, administrative, statutory, and common law controls. The concept of ownership is further complicated by two federal court cases that hold that the patient has a limited "property right" in the record.[49] However, most court cases reflect the patient's right to access the medical record and the medical information therein rather than their ownership rights to the physical record.

CONFIDENTIALITY AND PRIVACY OF MEDICAL RECORDS

The medical record is apt to contain more personal information than any other single document. It contains not only sensitive health care information, but also demographic, sexual, behavioral, dietary, and recreational information. Because of the vast amount of highly sensitive information in the medical record, patients have the expectation that the information therein will be held in privacy. That loss of personal privacy is the greatest concern of over a quarter of our population. [50]

The Privacy Versus Confidentiality Conflict

Patient privacy advocates look for a model based on access only by informed patient consent and question the need to circulate the health care information beyond the health care provider. Professor Alan Westin[51] defines this concept as "privacy."

On the other hand, Westin defines as "confidentiality" the question of how medical data shall be held and used by the provider that collected it, what other further uses will be made of it, and if or when the patient's consent will be required. The confidentiality advocates, hospitals, insurers, managed care organizations, educators, researchers, public health agencies, government agencies, utilization review organizations, and risk managers, hold to the premise that access to and sharing of health care data are critical to a well-functioning, cost-efficient health care system, and essential to the discovery and monitoring of disease trends.

The conflict between the concepts of "privacy" and "confidentiality" then, reduced to its basics, is whether we support privacy, recognizing that the greater social good will be negatively affected, or do we feel that the greater social good is important enough to negatively impact the privacy of the medical records and the information therein. There appears to be little doubt that current legal theory supports the concept of confidentiality, and in this day of third-party payers, fourth-party auditors, and the multiple legitimate needs for health care information, classical patient privacy is a myth.

Constitutional Privacy Protections

Privacy advocates relying on constitutional privacy protection get little support. First, the right to privacy under the

Constitution offers protection only from intrusions by the government.[52] Therefore, constitutional remedies do not reach breaches by private health care information holders. Further, a whole series of federal court cases have demonstrated that even when there is government intrusion into individually identifiable health care information, individuals cannot rely on constitutional protections to preserve their privacy. The strong public interest represented by the need for the information outweighs the individual's need for privacy. The seminal case in this series is *Whalen v. Roe*.[53] In an attempt to stem the illegal distribution of prescription drugs, the New York legislature passed a law requiring all prescriptions for Schedule II drugs to be logged and information concerning the prescription, including the identity of the patient, to be transmitted to the State Department of Health. Public disclosure of the information was forbidden and access to the information was confined to department and investigative personnel. Patients receiving Schedule II drugs and their doctors brought suit questioning the constitutionality of the law. They argued that the doctor–patient relationship was one of the zones of privacy accorded constitutional protection. A unanimous United States Supreme Court held that the patient identification process was reasonable exercise of the state's broad police powers.[54] In *United States v. Westinghouse Electric Corp*.[55] the United States Court of Appeals for the Third Circuit elucidated the following seven factors to be considered in determining "whether an intrusion into an individual's privacy is justified . . .":

- the type of record requested;
- the type of information it does or might contain;
- the potential for harm in any subsequent nonconsensual disclosure;
- the injury from disclosure to the relationship in which the record was generated;
- the adequacy of safeguards to prevent unauthorized disclosure;
- the degree of need for access;
- whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[56]

The test appears to have survived the test of time[57] and offers pragmatic evidence that even under constitutional protections privacy is dead and confidentiality reigns.

Confidentiality

Section 5.05 of the AMA Code of Ethics adopts a standard for confidentiality.[58] It directs the physician not to reveal information about the patient without the patient's consent or as required by law. It then goes on to say some "overriding social considerations" will make revelations "ethically and legally justified." While the text and the 65 annotations may give a member physician some idea of the scope of the problem, the broadness, vagueness, and double-speak of Section 5.05 reflect the current confused state of medical record confidentiality in the United States.

State Regulation

State statutes have developed piecemeal across the country. All states require health care providers to report some types of patients to state agencies.[59] However, universality ends with that statement. State confidentiality rules are dramatically inconsistent in their regulations and even their presence.[60] Ohio appears to be the only state with an independent tort for unauthorized disclosure of medical information.[61] In general, states have been largely unsuccessful in finding ways to compensate patients for injury sustained by authorized disclosures.[62] In pre-World War II America this was not a problem. The population was not tremendously mobile and health care information was essentially local. However, since World War II the American population has become increasingly mobile, and coincident with both that mobility and the development of regional and national payers, health care information has crossed state lines as never before. In addition, the expanded use of electronic health care information has no regard for state boundaries. The patchwork effect of strikingly different state confidentiality regulations, or complete lack thereof, became a major problem. Both UHCIA and HIPAA developed in response to this problem.

Privacy and Confidentiality of Electronic Medical Records

The privacy issue is the most common concern voiced about electronic medical records. Privacy can no longer be a consideration in medical records of any type. What the health care industry must consider are reasonable rules of confidentiality. Electronic records have all the confidentiality concerns of their paper counterparts and the added concerns of preserving the integrity of the record and preventing unauthorized remote access to the information. Although medical record security in general has been discussed above, some issues specific to the security of electronic records are discussed below.

Access

With paper records one of the principal security measures employed is limiting access to records to a limited number of individuals and, in some situations, limiting access to only the attending physician. However, one of the great advantages of the electronic medical record is that it can offer seamless recording from any number of sources. It can also offer access to a nonfragmented medical record to the same number of sites. Therefore, traditional criteria of limiting access to a single physician or group of physicians or limiting access by job criteria will limit the benefits of the electronic record. All providers involved in the care of the patient should have access to and be able to record in the record. It is as important for the dentist caring for the patient to know about the patient's rheumatic fever as it is for the pharmacist or clinical pharmacologist to know about the patient's renal function. When the patient comes to the Emergency Department in the middle of the night, the triage person needs immediate access to the complete record. This means access must be spread across a wider

range of provider and job categories and cannot be limited by current "attending" criteria.

Authorizations

The access issues described above mandate that a system of blanket category authorizations to enter the system must be made. For instance, "all licensed providers" (which would include LPNs in many states); or "all licensed providers except..."; or "all licensed providers and...."

Authentication

In the field of electronic medical records, authentication is defined as the system for determining the identity of an individual seeking access to the system to enter or retrieve data. The simplest authentication system is the combination of user identification name and password. If the individual enters that combination of symbols making up the user name followed by the proper password, entry is allowed. User identification names are usually permanent and are frequently numerical. Passwords are generally changed periodically, monthly, or quarterly. Another relatively simple system combines the user identification name with a smart card not unlike a credit card or mechanized gate card. As computers have become more sophisticated, so have authentication systems. Commercial authentication systems are now available based on "digital signature," fingerprints, retinal patterns, facial biometrics, and voice recognition. Authentication systems need constant upkeep to remove people who leave the system and add people new to the system.

Firewalls

Another advantage of electronic records is that they allow remote access to medical records. Therefore, providers may access and enter data from remote sites such as physician offices and outlying clinics. The access ports for these remote sites are vulnerable to unauthorized individuals entering the system. They must be guarded by firewalls. A firewall is a point of entry for remote users that can be configured and controlled. A firewall normally restricts access by denying entry to incoming messages arising from an unapproved source, and limiting access to approved sources such as a list of approved phone numbers or identified computers. A firewall may also limit the functions it allows an incoming source to perform.

Transmission Control Protocol Wrappers

Wrappers serve somewhat the same function as firewalls. Wrappers may be thought of as functioning within the server rather than at the port of entry, as does the firewall. It too will intercept incoming data and check it against a programmed security protocol. Wrappers can not only deny entry to the system or prevent a proposed function, but can audit the source, date, and time of the entry.

Audit Trails

As has been discussed above, an audit trail (a.k.a. audit log) logs all access to electronically stored medical information. An effective audit trail will record not only the identification of the individual accessing the record and the time and date of record access, but also the record or records accessed, the portion of the record accessed, and the action made. The audit trail must be secured against modification and provide for periodic analysis for unauthorized access. Audit trails that meet or exceed these criteria appear to be an effective tool in preventing unauthorized access to records.

Under HIPAA final rules,[63] the patient has the right to request a log of disclosures made for the 6 years prior to the date of the request. That log must contain: the date of disclosure; the name of the entity or individual who received the protected health care information and, if known, their address; a brief description of the health care information disclosed; a brief statement of the purpose of the disclosure or, in lieu of the statement, a copy of the written request for the information.[64] Routine disclosures for the purposes of treatment and care are excepted from this disclosure mandate, as are certain disclosures protected by other HIPAA sections.[65]

Encryption

If health care information is to be sent over public networks such as the World Wide Web, it should be encrypted to ensure confidentiality.

Virus Control

Viruses must be controlled by strict rules against downloading unauthorized software programs from the web or bringing in software from home. In addition, antivirus software must be installed and updated on a regular basis. Regular checks of the software configurations and unauthorized service ports will help control the problem as well.

PCASSO

A brief review of the University of California at San Diego Healthcare's Patient-Centered Access to Secure Systems Online (PCASSO)[66] will give the reader a sense of how all the factors mentioned above come together to develop a reasonably secure system with patient and multiple provider access. PCASSO was conceived to empower patients to become active participants and partners in their health care, while satisfying the state and federal regulations (including HIPAA) and the University's IRB. The plan utilizes the Internet to allow both patients and providers to access records from almost anywhere, if they elect to become part of the PCASSO program. Patients are asked to sign the following consent before being enrolled in the program:

> *The information you will be able to access via the PCASSO system is technical and contained in systems that were originally designed for trained health professionals to use only. As a result, there is a possibility that you will be exposed to information that you do not understand or find startling. PCASSO is not intending to place upon you the burden of interpreting your medical record, nor to cause you to act on the information received without first discussing it with your physician. One of the risks associated with this study is that "a little knowledge is a dangerous thing." By agreeing*

to participate, you agree to contact your physician to help to resolve any questions or problems that might arise as a result of viewing your medical data online. If you have difficulty contacting your physician, you may contact PCASSO project staff, who will assist you in contacting your physician.[67]

In addition, a hotline and triage system was established to take care of any questions for distraught patients. Such calls were classified as information toxicity and reported to the IRB.

Patients' clinical data is entered into the program's server as divided messages classified as to sensitivity level, as low, standard, public deniable, guardian deniable, or patient deniable. "Low" data is not patient identifiable.[68] "Standard" is health information that is patient identifiable and does not fall into any of the deniable categories. "Public deniable" is information protected by special state or federal statute such as mental health, AIDS and HIV infections, abortion, adoption, substance abuse, and sexually transmitted diseases (STD). "Guardian deniable" is information that can legally be withheld from a guardian about a minor patient, such as abortion, STD, or substance abuse in some states. "Patient deniable" is information that the primary physician believes is capable of causing harm to the patient if it were disclosed to that patient, most often psychotherapy notes.

A firewall separates PCASSO from the remainder of the university system. The user logs in from any of the common web browsers and uses a graphical image keyboard and a combination of authentication procedures, a password, a token, and a public–private key pair. The private key is a diskette that interacts with the server and mutually authenticates the communicators. (In some states such disks include the encryption program. In others the encryption program is downloaded as part of the setup procedure.) An individually held plastic card with a serial number is the final step in the authentication process. If the name, password, number, and key correspond, entry is permitted. A technical support number is available if entry or other problems are encountered. All PCASSO operations are monitored and logged, including any attempted penetrations. Its designers believe it meets all the criteria required by HIPAA.[69] It allows for emergency access, role-based access, encryption, access (including unauthorized attempts) audits and logs, unique identifiers plus password and token, automatic log off, and technical and informational support.

With authentication completed, a screen customized for patient or provider appears. PCASSO's secure communication system allows authorized patients and providers to access specific information and for the providers to carry out privileged additions to the record. PCASSO does not allow the information to be saved to disk, printed out, or transferred to another application. In many ways the system seems more secure than allowing patients to view paper records. Information labeled "pending" or "interim" is filtered out.

PCASSO was fully operational by the spring of 1999. The system has been judged safe and effective as a medical device by the FDA.[70] The system has repulsed all efforts of hackers, first by security consultants and then by hackers at large. Extensive review by risk managers and the California University System's attorneys concluded that the benefits of the system far outweighed the risks. In practice, a greater percentage of patients used the system than did physicians. Patients thought the access precautions very reasonable while many of the physicians considered them unreasonable or intolerable. However, a majority of both the physicians and patients thought the value of having the records available on the Internet was very high.

In conclusion, PCASSO and, by inference, electronic record systems like it, will provide secure electronic records available to both patients and providers. However, high security, while acceptable to patients, has come at a perceived increased price in time and effort to the provider.

PRIVILEGE AND ADMISSIBILITY

Provider–Patient Privilege

An issue closely related to privacy and confidentiality is how confidential health care information is treated by the courts. As might be surmised from the discussions above, it would seem apparent that nowhere is the release of confidential health care information more in the public interest than in the court of law. In addition, there is no doctor–patient testimonial privilege in the common law. It therefore seems incongruous that since 1828 all but three states have passed some sort of provider–patient testimonial privilege statute.[71] The statutes vary widely from state to state but all offer some degree of protection to the patient by not allowing the provider to testify in court about the patient's medical information. Many states do not recognize the privilege in criminal cases, others limit the privilege to psychotherapists, and others include a variety of health care providers in addition to physicians. Under Section 501 of the Federal Rules of Evidence, if a claim in a federal court arises under federal law, no privilege will be recognized.[72] There has been a definite trend in both federal and state courts to look at the health care testimonial privilege skeptically. Even in that bastion of privilege, the psychiatric record, courts have questioned the merits of confidentiality. Critics see the privilege as nothing more than a litigation tactic and doubt that testimony deters people from seeking psychiatric or, for that matter, any health care. The current uses of group therapy and the fact that people in states without privilege seek care at the same rate as in privilege states are frequently asserted arguments.

Nonetheless, a general body of law has developed in regard to the provider–patient privilege. The privilege extends to the entire medical record, including x-rays, laboratory reports, billing records, and all other documents compiled and maintained by the provider.[73] The communication must be made in confidence for the privilege to apply. The communication must also be made within the context of the provider–patient relationship and be made in regard to diagnosis or treatment. Therefore, situations in which the communicator is a nontraditional patient, such as one undergoing an independent medical examination, or relating facts unrelated to diagnosis or treatment, are not covered by the privilege.[74]

The privilege and the benefit thereof belong to the patient, although anyone with an interest may assert it. Only the patient may waive the privilege. The waiver may be express or implied. An express waiver is made when the patient signs an authorization directing the provider to disclose the information. Implied waivers may be made in several different ways. The patient may voluntarily introduce the medical evidence to the court; the patient may voluntarily place his or her medical condition at issue in litigation; or the patient may fail to assert his or her privilege when the medical information is placed into evidence. A good rule of thumb for health care providers is always to assert the privilege when faced with a subpoena that is not accompanied by a patient's authorization to disclose the information. As we have mentioned above, this is required by the federal alcohol and drug regulations and even in cases not involving alcohol or drugs, failure to assert the privilege has resulted in liability in at least one state court.[75]

Admissibility

As is the case with all evidence, medical records must be relevant and material to the issues before the court to be admitted into evidence. However, depending on the document, a variety of objections may be raised to the admission of even relevant and material health care information. In addition to the privilege objection discussed above, some medical information, such as incident reports, may be protected because they were made in anticipation of litigation or fall within the attorney–client privilege or are part of the attorney's work product. However, the most often used objection to admission is that the medical record is hearsay. It is an out-of-court statement being introduced to prove the truth of the matter asserted in the statement. However, medical records tend to fall into one of a number of exceptions to the hearsay rule. First, medical records are business records or records [76]of regularly conducted activity and fall under that exception in the hearsay rule.[77] Second, statements made for the purposes of medical diagnosis or treatment[78] are exceptions to the hearsay rule. Finally, dying declarations[79] and declarations against interest[80] are also exceptions that may apply to medical records. For practical purposes, records made in accordance with the record-keeping mechanics outlined above will be admitted as evidence over the hearsay objection.

Acknowledgement

S.Sandy Sanbar, Chairman, Textbook Editorial Committee, combined and edited two chapters on paper and electronic medical records, which were authored by Fillmore Buckner MD, JD, FCLM, in the 6th edition.

Endnotes

1. HIPAA regulations on electronic billing practices are covered under 45 C.F.R. Parts 160 and 162. Strangely, the Centers for Medicare and Medicaid Services' *Business Partner's Security Manual* still restricts any Internet health care claims, §5 Internet Security Rev. 02-13-02.
2. *See* Heinze et al., *Mining Free-Text Medical Records*, 254 AMIA Annual (2001).
3. *See* Haskins, *Legible Chart*, 48(4) Canadian Family Physician 768 (2002).
4. *See* van Wingerde et al., *Linking Multiple Heterogenous Data Sources to Practice Guidelines*, 391 AMIA Annual (1998).
5. *See* Kapp, *Our Hands Are Tied: Legal Tensions and Medical Ethics* (Auburn House, Westport, Conn. 1998).
6. See Evans et al., *Preventing Adverse Drug Events in Hospitalized Patients*, 28 Ann. Pharmacotherapy 523 (1994).
7. *Id*. at 523.
8. *See* F. Buckner, *The Duty to Inform, Liability to Third Parties and the Duty to Warn*, 100 J. Medical Practice Management (Sept./Oct. 1998).
9. *See* Loomis et al., *If Electronic Medical Records Are So Great, Why Aren't Family Physicians Using Them?*, 51(7) J. Family Practice 36 (2002).
10. *See* Washington Administrative Code, Title 246: Department of Health §246-318-440: Records and Reports—Medical Record System.
11. Joint Commission on Accreditation of Healthcare Organizations, *Accreditation Manual for Hospitals*, Standards 5–10, 54–63 (1995).
12. 42 C.F.R. Ch. IV §482.24.
13. Rule 803(6), Federal Rules of Evidence for United States Courts and Magistrates Effective July 1, 1975 as Amended to September 1, 1991 (West).

    (6) ***Records of Regularly Conducted Activity.*** *A memorandum, report, record, or data compilation, in any form of acts, events, conditions, opinions or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity. . .*

14. From Apgood, *Electronic Evidence*, 53(8) Washington State Bar News 46, 47 (1999).
15. *See* Rule 34, Federal Rules of Civil Procedure; *see also* Rule 803(6), Federal Rules of Evidence, *supra* note 13.
16. Rule 1001(3), Federal Rules of Evidence, *supra* note 13.
17. *Bray v. Bi-State Development*, 949 S.W. 2d 93 (1997).
18. National Conference of Commissioners on Uniform State Laws, *Uniform Health Care Information Act*, 9 U. La. Ann. 478 (1988).
19. *Id*. §4-102.
20. *Id*. §4-101; DHHS Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§160–164 10-1-01, Final rule, Federal Register, Aug. 14, 2002, 67(157):53182–53273, to be codified at 45 C.F.R. Parts 160–164; §3-102 UHCIA, *supra*; 45 C.F.R. §164.524 10-1-01 edition, *supra* (note this section was not changed in the final rule of August 2002.); §3-102 UHCIA, *supra*; 45 C.F.R. §164.524 10-1-01 edition, *supra* (note this section was not changed in the final rule of August 2002).
21. For examples, *see* Wn. Rev Code 70.02.080 (1993); Fla. Stat. Ann. §455.241 (1985); Or. Rev. Stat. Ch. 192 §525 (1993); Nev. Rev. Stat. Ch. 629 §061 (1983); N.Y.M.H.L §33.16 (1988).
22. §4-101 UHCIA, *supra*; 45 C. F. R §164.526 10-1-01 edition, *supra* (note this section was not changed in the final rule of August 2002).
23. §§8-101, 8-102, 8-103, UHCIA, *supra*.
24. Pierce v. Penman, 515 A. 2d 948 (1986).
25. *Thor v. Boska*, 113 Cal. Rptr. 296, 302 (1974).
26. *See* Anderson: *Counterfeit, Forged and Altered Documents*, 32(6) Law Society J. 48 (1994); Fortunato & Steward, *Sentence Insertion Detected Through Ink, ESDA, and Line Width*, 17 J. Forensic Sciences 1702 (1992); Schwid, *Examining Forensic Documents*, 64 The Wisconsin Lawyer 23 (1991).

27. *See* Model Penal Code §241.7
28. F. Buckner, *Cedars-Sinai Medical Center v. Superior Court and the Tort of Spoliation of Evidence*, 6(1) Legal Medicine Perspectives 1–3 (1999).
29. *Ritter v. Board of Commissioners of Adams County Public Hospital*, 637 P. 2d 940 (1981). *See also* F. Buckner, *Medical Records and Physician Disciplinary Actions*, 11 J. of Medical Practice Management 284–290 (1996); H. Hirsh, *Tampering with Medical Records*, 24 Med. Trial Tech. Q. 450–455 (Spring 1978); Preiser, *The High Cost of Tampering with Medical Records*, Medical Economics 84–87 (Oct. 4, 1986); Gage, *Alteration, Falsification, and Fabrication of Records in Medical Malpractice Actions*, Med. Trial Tech. Q. 476–488 (Spring 1981); Mich. Stat. Ann. §14.624(21) (Callaghan 1976); Tenn. Code Ann. §63-752(f) 14 (Supp. 1976); Tenn. Code Ann. §39–1971 (1975) (making it a crime to falsify a hospital medical record for purposes of cheating or defrauding).
30. In at least one state, such statutes of repose have been struck down making the discovery rule applicable indefinitely. *DeYoung v. Providence Medical Center*, 136 Wn. 2d 136; 960 P. 2d 919 (1998).
31. Several states specifically authorize the microfilming of records. *See* Cal. Evid. Code §1550 (West 1986).
32. F. Buckner, *Closing Your Medical Office*, 4 J. Medical Practice Management 274–280 (1989).
33. Medicare and Medicaid Guide (CCH) ¶6420.85 (1990).
34. 42 C.F.R. §482.24(b)(1) (1990).
35. *Id*.
36. 21 C.F.R. §291.505(d)(13)(ii).
37. 21 C.F.R. §291.505(f)(2)(v).
38. 29 C.F.R. Chap. XII, §§1904 et seq.
39. Joint Commission on Accreditation of Healthcare Organizations, *Accreditation Manual for Hospitals* (JCAHO, 1990), Standard MR 4.2.
40. American Hospital Association and American Medical Record Association, *Statement on Preservation of Medical Records in Health Care Institutions* (1975).
41. *See* Tenn. Code Ann. §68-11-305(c) (1987).
42. 42 C.F.R. §2.16.
43. *Id*.
44. §164.530(c) (1 and 2), Standards for the Privacy of Individually Identifiable Health Information, *supra* note 10; §7-101, UHCIA, *supra* note 18. *See also* discussion on HIPAA (Chapter 16 this volume).
45. *See Fox v. Cohen*, 406 N.E. 2d 178 (1980); *Bondu v. Gurvich*, 473 So. 2d 1307 (1985).
46. Dewitt et al., *Patient Information and Confidentiality: Treatise on Health Care Law* (Mathew Bender, 1991).
47. *Parsley v. Associates in Internal Medicine*, 484 N.Y.S. 2d 485 (1985).
48. *See* Tenn. Code Ann. §68-11-304 (1990).
49. *See Bishop Clarkson Memorial Hospital v. Reserve Life Insurance, Co.*, 350 F. 2d 1006 (8th Cir. 1965); *Pyramid Life Ins. Co. v. Masonic Hosp. Assn.*, 191 F. Supp. 51 (W.D. Okla. 1961).
50. Wall Street Journal/ABC poll of September 16, 1999, quoted in *Standards for Privacy of Individually Identifiable Health Information: Proposed Rule*, 64 Federal Register 59917 (Nov. 3, 1999) at 59919.
51. Alan Westin, *Computers, Health Records and Patient's Rights* (1976).
52. Barefoot, *Enacting a Health Information Confidentiality Law: Can Congress Beat the Deadline?*, 77 N.C. Law Rev. 283 (1998).
53. 429 U.S. 589 (1977); *see also U.S. v. Miller*, 425 U.S. 435 (1976).
54. *Id*. at 598–604.
55. *United States v. Westinghouse Electric Corp*., 638 F. 2d 570 (1980).
56. *Id*. at 578.
57. *See Doe v. Southern PA Transportation Authority*, 72 F. 3d 1133 (1995).
58. AMA Council on Ethical and Judicial Affairs, *Code of Medical Ethics: Current Opinions and Annotations*, §5.05 (1997).
59. F. Buckner, *The Uniform Health-Care Information Act: A Physician's Guide to Record and Health Care Information Management*, 5 J. Medical Practice Management 207 (1990).
60. *See* §1-101 UHCIA, *supra* note 16; *see also* Barefoot, *supra* note 52.
61. *Biddle v. Warren General Hospital*, 715 N.E. 2d 518 (1999).
62. *See generally* Frankel, *Do Doctors Have a Constitutional Right to Violate Their Patient's Privacy?*, 46 Villanova Law Rev. 141 (2001).
63. 45 C.F.R. §164.528 10-1-2001 (Modified Federal Register 67(157) at 53271).
64. *Id*. at 53272.
65. *See* 45 C.F.R. §§164.502, 164.510, 164.512.
66. Masys et al., *Giving Patients Access to Their Medical Records Via the Internet*, 9(2) J. American Medical Informatics Association, 181 (2002). *See also* Masys et al., *A Secure Architecture for Access to Clinical Data Via the Internet*, MedInfo 1130 (1998–99); Baker & Masys, *PCASSO: A Design for Secure Communication of Personal Health Information Via the Internet*, 54(2) Int. J. Medical Informatics 97 (1999).
67. *Id*. at 186.
68. *See* 45 C.F.R. §164.502(d).
69. Masys, *supra* note 66, at 183.
70. *Id*. at 184.
71. South Carolina, Texas, and Vermont.
72. Rule 501, General Rule, Federal Rules of Evidence for United States Courts and Magistrates Effective July 1, 1975 as Amended to September 1, 1991 (West).
73. *See Tucson Medical Center v. Rowles*, 520 P. 2d 518 (1974).
74. *See Polsky v. Union Mutual Stock Life Ins. Co*., 436 N.Y.S. 2d 744 (1981); *see also Chiasera v. Mutual Ins. Co*., 422 N.Y.S. 2d 341 (1979); *Griffths v. Metropolitan St. Ry. Co*., 63 N.E. 808 (1902).
75. *Smith v. Driscoll*, 162 P. 572 (1917).
76. *See* Fla. Stat. Ann. §90.803(6).
77. Rule 803(6), Federal Rules of Evidence, *supra* note 72.
78. *Id*., Rule 803(4).
79. *Id*., Rule 804(b)(2).
80. *Id*., Rule 804(b)(3).