



# CCHIT Certified Electronic Health Records and other Safety Enhancing Technologies

Medical Legal Risk Management Benefits, Pitfalls and Safeguards

## **Introduction: Requirements for Medical Legal Liability**

### Duty

In law, there are “duties” between and among individuals not to engage in certain behaviors, or to act (or fail to act) in such ways which may unreasonably cause physical and/or emotional harm or distress. This is the basis of negligence or tort law. Medical liability (sometimes known as medical negligence or medical malpractice) is a special component of tort law. It governs the professional relationship between physicians and their patients. Medical liability law concerns the duties of care expected between physicians and their patients in delivering health care. A physician’s duty to his or her patients is to practice medicine which meets or exceeds the standard of care. Once a physician-patient relationship is established, the physician’s general duty is to provide that level of care expected of a reasonably competent physician (*Tan, SY Medical Malpractice: Understanding the Law, Managing the Risk. Hackensack, NJ: World Scientific; 2006:37*)

### Breach of the Standard of Care

The crux of a medical liability action concerns whether it can be demonstrated by the “preponderance of the evidence” that a physician has violated or deviated from the standard of care. As a rule, expert testimony from a physician of the same or similar specialty is required to establish the standard of care and that a defendant physician deviated from it. Where alternative proper methods of treatment exist, there is no deviation from the standard of care if a physician chooses one method over another and an injury results (*Bennett v. United States, 2006 U.S. Dist. LEXIS 10966, at 39 (N.D., Ill. Feb. 24, 2006)*). Some states, notably Maine and Kentucky, have passed legislation allowing physicians the choice of being covered by practice guidelines, with compliance constituting evidence against an allegation of negligence (*Maine Rev. Stats. Ann. Sect. 2975; Kentucky Rev. Stat. Sect. 342.035*)

## Preventable Injury/Legal Cause in Fact

For there to be any medical liability action, there must be an injury to a patient (of a physical, mental or emotional nature) that could and (more likely than not) would not have occurred (i.e. it was preventable) in the absence of the physician's deviation from the standard of care. In other words, the physician's deviation from the standard of care (constituting negligence) must have constituted the legal cause in fact of the patient's injury.

## Proximate Causation

Establishing causation does not require a plaintiff to prove that the negligent act or omission is the sole cause only that it is a "proximate cause" of the alleged (otherwise preventable) injury. It is not sufficient to show merely that an injury occurred; evidence of a bad result does not constitute evidence of lack of skill or negligence. (Bennett, 2006 U.S. Dist. LEXIS 10966, at 38). The patient's injury must be the "reasonably foreseeable" natural consequence of the physician's negligence (or deviation from the standard of care) to meet the requirements of proximate cause in proving the substantive merits of a medical liability action.

## Resultant and Recoverable Damages

The injury to the patient which is the foreseeable natural consequence of the physician's deviation from the applicable standard of care (which was his or her duty to the patient to meet) still must result in measurable damages. These may be comprised of past, present and/or future medical expenses and other economic setbacks such as loss of employment and other costs. In addition, there may be the much less quantifiable,

but often even larger, "pain and suffering" non-economic damages (which may be capped at a certain dollar amount, e.g. anywhere from \$250,000 to \$1,000,000 depending on prevailing state law).

If there is no lasting disability resulting from the negligence, or if the disability is small, the award may not be large enough to warrant the expense of pursuing the case. Cases where larger sums are at stake are likely to be contested more aggressively. Cases where negligence may be more obvious but which have less at stake may not be pursued as aggressively or be settled more expeditiously (Franklin, C, Marutzky, EM, Sandberg, CM, *Medical Professional Liability: Physicians' Guide to Understanding Professional Negligence Claims; Resident and Staff Physician; 53(7):22-25 (July/August, 2007)*)

---

## Types and Theories of Liability

### Institutional Liability and Causes of Action

#### **Corporate Liability for Organizational Negligence**

In addition to the individual negligence theories discussed immediately above which could involve physicians using electronic health records and other safety enhancing technologies, there are also corporate/enterprise or organizational theories of liability. Most of these actions in the past have involved holding hospitals liable for inadequate oversight of staff physicians. However, hospitals (as well as their physicians) might become the subject of corporate negligence actions if a hospital violated the standard of care (through inadequate oversight of its staff physicians) by allowing an electronic health record or other technology of its

choosing to be used in such a way to cause harm to patients.

### **Vicarious Liability for Vendor/User Negligence**

A corollary to the corporate liability theory of liability discussed immediately above could be that of vicarious liability. If there is a design or other type of flaw in an electronic health record or other technology (e.g. computerized physician order entry) which results in harm to patients (even though the physicians or other caregivers using it committed no negligence which may have been foreseen or prevented by the hospital), then the hospital might still be held liable for having chosen this particular vendor product. The hospital might be able to recoup its losses from the vendor in such a situation, but that would still involve considerable time and legal expense to do so.

### **Privacy Violations**

One of the biggest potential sources of liability in the use of electronic health records may derive from actions alleging violations of privacy. There have already been several highly publicized events involving the accidental leaking of electronic private medical information of patients of the Veterans Health Administration, major health plans and delivery systems. These leaks may result from inadequate security precautions by the holders of these electronic databases and/or design flaws in the systems intended to block access to all but password protected users. The specter of security breaches has proven to be one of the major speed bumps impeding the more widespread use of electronic health records and other safety enhancing technologies in the U.S.

## **Other Causes of Action involving Individuals Using Electronic Health Records**

### **Acts of Commission**

Medical liability (as well as other tort or civil law) actions may arise from acts of commission which breach the standard of care and result in injury and damages to patients as discussed above. One type of act which physicians might commit concerning electronic health records that could involve them in litigation is to turn off the clinical alert systems designed to prevent unsafe treatments. One recent study found that drug safety alerts were being overridden by clinicians in 49% to 96% of cases (*Van Der Sijs, H, et. al.: Overriding of Drug Safety Alerts in Computerized Physician Order Entry; Journal of the American Medical Informatics Association; 13(2): 138-147 (2006)*)

### **Acts of Omission**

Physicians could also find themselves in legal hot water by failing to use diagnostic and treatment modalities suggested by the embedded best practice guidelines in certain types of electronic health records. Here there could be an act of omission contributing to patient injury.

---

## **Prevention of Liability through CCHIT Certified Electronic Health Records and other Safety Enhancing Technologies**

Promoting Improved Quality of Care and Medical Legal Risk Management

### **Improved Aggregation, Analysis and Communication of Patient Level Information**

One of the biggest causes of medical liability actions is the failure to consider all aspects of the patient's condition prior to making diagnoses, or decisions to hospitalize, discharge, or to obtain additional tests, procedures or consultations. To become certified by the Certification Commission for Healthcare Information Technology (CCHIT<sup>SM</sup>), electronic health records in both the ambulatory and inpatient settings must address this issue.

According to CCHIT Commissioner and Family Practice Associates of Lexington administrator, Susan Miller: "...At a minimum, to be certified, electronic health records must demonstrate their complete functionality by ensuring that the record is complete, accurate, secure and interoperable with other systems from which it must obtain additional information about the patient." This benefit of CCHIT Certified<sup>SM</sup> electronic health records alone would be enough to justify their costs from the perspective of defense attorneys who have lost or settled cases due to the woefully inadequate, incomplete, widely scattered and often illegible handwritten medical records.

### **Diagnostic Decision Support**

Another of the biggest causes of medical liability actions continues to be that of missed, inaccurate and/or delayed diagnoses. The results of a fairly recent study published in the "Journal of the

American Medical Association" which was cited in a February 22, 2006 article in the "New York Times", found that there has been no significant improvement in diagnostic decision making overall since the 1930s! In spite of the tremendously more accurate diagnostic technologies now at the disposal of the nation's physicians, without complete, accurate, legible information on the patient in an understandable, quickly assessable, format, it is just as difficult to diagnose patients now as it was in the 1930s. Physicians (especially those on referral) can't readily evaluate what has been done, why, what the results were and how what they can do now can further the diagnostic process.

CCHIT Certified electronic health records may provide significant help in the diagnostic process, not only by providing all the relevant information on patients' findings in one place. These records also provide ongoing alerts concerning the results of follow up tests, procedures and consultations to provide the most up to date, complete and accurate information needed to make timely, correct diagnoses.

### **Therapeutic Decision Support**

Another major reason for liability arises from the inability sometimes of even the most accomplished clinicians to be able to make the best evidence based decisions at the point of care supporting optimal therapy for their patients. The long standing promise of clinical decision support systems (hereafter CDSS) cannot be fulfilled without the integration of these with CCHIT Certified electronic health records.

The sum total of medical knowledge is doubling every couple of years. This exponential increase requires the ability to access at or near the point of care best evidence based practices electronically. CCHIT Certified electronic health records can provide both the electronic input of the necessary patient information and the

integration with other functions to optimize the usefulness of CDSS.

All electronic entries are time and date “stamped.” Clinicians making entries are identified and their role is defined. These features alone constitute tremendous risk management benefits of CCHIT Certified electronic health records, according to Dr. Abha Agrawal, CCHIT Commissioner and Chief Medical Information Officer of Kings County Hospital in Brooklyn. These capabilities will permit the faithful reproduction of the clinical decision making process to aid in the medical defense of cases far more effectively than scattered, incomplete, illegible paper records and faulty memories ever could.

### **Prevention of Adverse Events**

As an important adjunct function to aid in clinical decision making, CCHIT Certified electronic health records also will keep physicians from going down unsafe pathways. They accomplish this through built in guards against prescribing drugs and other treatments which (based on a patient’s current medications, lab results including kidney function, body weight, allergies and other factors captured in the electronic database on that patient) would result in adverse events.

These capabilities alone (so long as they are used fully by physicians) justify the use of CCHIT Certified electronic health records. They also facilitate the required knowledge transfer during hand offs across care settings so often at the root of patient injuries. This is all a part of the portability of electronic records which CCHIT Certified electronic health records promote.

### **Clinical Alerts and Reminders**

Not getting the latest indicated screening tests to detect potentially life threatening conditions in their early, treatable forms (e.g. cancers or heart disease) or adequately monitoring chronic ailments to prevent their complications (e.g. diabetes) has always been a major source of liability

claims. With the growing list of ever more sophisticated tests and procedures now available for this purpose, this allegation of malfeasance will only become more prevalent in the future.

A very valuable feature of CCHIT Certified electronic health records is their ability to produce reports on patients who meet certain criteria. These reports can be used to create a “registry” of patients with diagnosed conditions requiring careful monitoring to prevent complications (e.g. diabetes, asthma, etc.) or those who (because of age and other factors) need to be screened to prevent cardiac events or growing cancers, among other conditions. This provides yet additional risk management benefits in this important area for physicians according to CCHIT Commissioner and Vice President of McKesson Practice Partner, Andrew Ury, M.D.

### **Disclosure of Elements Promoting Informed Consent**

Although not usually a primary allegation in litigation, the failure to provide and document proof of informed consent for treatments and procedures can severely hurt the medical defense of any case. CCHIT Certified electronic health records can electronically memorialize the key elements of informed consent, viz.:

- The nature of the patient’s condition;
- The key aspects of the proposed procedure and why it is necessary to evaluate and/or treat this condition;
- The risks associated with this procedure;
- The available alternatives;
- The likelihood of success of the proposed procedure and its major alternatives; and
- The prognosis for the patient if nothing is done.

### **Electronic Record for Clinical Quality Improvement Research**

The standard of care especially for the diagnosis and treatment of certain conditions (especially heart disease and cancers) is constantly changing and getting more difficult to meet. There is an unrelenting need to improve continuously just to keep ahead of the ever rising standard of care—hence the need to engage in clinical quality improvement research.

Whether or not this is done in a formal manner (as might occur at a university), constantly monitoring, evaluating and improving the care physicians deliver is increasingly demanded (by payers, patients, policymakers, and, unfortunately, plaintiffs' attorneys and their experts). CCHIT Certified electronic health records make this kind of clinical quality improvement research and monitoring far less labor intensive. It is another major benefit, which, in the near future, will have medical legal risk management value, also.

### **The Benefits of CCHIT Certified EHRs in Defending Medical Liability Cases**

#### **Demonstration of Adherence with Best Evidence Based Practices**

One of the most difficult challenges in defending medical liability cases is to be able to demonstrate that defendant physicians adhered to the best evidence based practice standards. With the rapidly growing national practice guideline movement, increasingly, courts are looking for proof of adherence with these national guidelines as evidence of meeting the standard of care.

In this area, using CCHIT Certified electronic health records may be of great value to the defense of liability actions. These electronic records may even alert physicians when best evidence based practices and clinical reminders are not

followed or heeded, according to Jane Metzger, CCHIT Commissioner and Director of Research for First Consulting Group, a leading Health IT consulting firm.

So long as physicians capitalize on the built in intelligence of these records by accessing these guidelines (or to electronically document the rationale for not following them), should they become involved in litigation, their actions (or inactions) will be much easier to defend.

#### **Complete, Legible Record Readily Available for the Defense**

Unquestionably, one of the biggest benefits of CCHIT Certified electronic health records to the defense is having in one place a complete, legible record on the patient (who may have become a plaintiff). This permits a much easier and more accurate reconstruction of exactly what happened in the care of the patient to justify the defense of the actions which were taken or not taken. This is especially beneficial to the defense where, as anticipated with CCHIT Certified electronic health records, these electronic records permit ready access to information collected from all the patient's individual and institutional providers. It is only then that any medical defense may proceed effectively.

---

## Medical Legal Pitfalls of Electronic Health Records

### New Federal Rules Permitting the Broad Discoverability of Electronic Records in Legal Actions

On December 1, 2006, the new Federal Rules of Civil Procedure approved by the U.S. Supreme Court prescribed what to produce, when and how with regard to the discovery of electronic records. According to the July 2, 2007 issue of "American Medical News" titled: "*Updating Digital Discovery: It's all on Record*", "...Before the rules changed... attorneys could request electronic information but might end up with a paper printout of an e-mail or PDF. This meant they couldn't search within the document or see the metadata, or background information, such as when it was created or where it was sent.

"Now, the rules make it clear that all electronically stored data is equally discoverable" and automatically included in a document request, said New York health lawyer Sean P. Dwyer, a partner with Havkins, Rosenfeld, Ritzert & Varriale, LLP. Although these rules are currently limited to federal causes of actions, state courts typically follow federal guidelines in developing their own rules. Once in state courts, these discovery rules will apply to medical liability actions. At least five states (Idaho, Kansas, Michigan, Montana and New Jersey) have already adopted discovery rules similar to these Federal rules.

In general, electronic health records are to be treated as "business records" so that they are admissible in legal actions under the business records exception to discoverability. Some electronic health records are not necessarily business records, and therefore, are not subject to evidentiary disclosure or discovery. These exceptions include, but are not limited to:

- Reproductions of electronic health records for convenience purposes (e.g. for infection control or other peer review committee meetings);
- Draft electronic documents (e.g. e-mail, voice mail, e-annotations, instant messages, etc.); or
- Personal Health Records (PHRs).

However, even these may be discoverable as business records if a provider used them to provide care, review data, or document observations or instructions.

Anticipating this new environment, the health care standards development organization (Health Level Seven or HL7) had released for public comment at the time of this writing the "Legal Electronic Health Record System Functional Profile", a guide that can "help an organization maintain an electronic health record for legal and business purposes." "It is important to know where to tweak the software to produce a Legal EHR, so that care can be tracked as a business record" according to Linda Kloss, CEO of AHIMA. Mark Leavitt, M.D., CCHIT chair, said for publication in the June 19, 2007 online edition of "Modern Healthcare" (<http://www.modernhealthcare.com>) in an article titled, "HL7 proposes Legal Angle to EHRs": "The EHR legal profile will become a part of future CCHIT criteria deliberations."

### Easily Demonstrable Deviations from Best Evidence Based Practices

Another potential medical legal pitfall where electronic health records are discoverable in a liability action is one in which the allegation is that a physician defendant either has turned off the clinical alerts or other best practice prompting reminders in a system, or otherwise ignored them. Physicians usually receive a "starter set" of clinical reminders, which physicians can either turn off or change (although those intended to prevent

adverse drug reactions can only have their sensitivities “toned down”). Physicians must realize that they proceed to a certain extent at their medical legal peril when they delete, change or otherwise ignore these safety features. Doing so may produce an easily discoverable audit trail for the plaintiff’s attorney in cases arising from failing to respond to those clinical alerts or easily accessible best practice guidelines.

Similarly, just as electronic health records can provide an easily accessible, complete and legible set of information concerning a patient’s care to justify what was done or not done (including illustrative graphics, digital photographs, videotapes and other audiovisual aids), so too may these be available for discovery by the plaintiff’s attorney and his or her medical experts. These may serve as equally compelling electronic documents and illustrations to the other side in establishing the failure to adhere to prevailing standards of care.

### Potential for Privacy Violations and Medical Identity Theft

Potential violations of patient privacy have proven to be one of the biggest “speed bumps” slowing the widespread adoption of electronic health records (or at least the willingness of federal agencies to subsidize their use). In the July 2, 2007 issue of “American Medical News” cited previously, according to Cynthia M. Stamer, a HIPAA privacy expert with Glast, Phillips & Murray, P.C., “....Federal HIPAA privacy protections pose a concern, because inadvertent disclosures can happen, particularly in a voluminous e-discovery request (see the discussion of e-discovery under the new Federal rules, above).

The federal rules of evidence, which prevent the disclosure of privileged information unrelated to the case at hand, do not trump the privacy protections, she noted. “You’re letting people walk through

your personal health information if you don’t have a system that divorces medical records from other business records,” Stamer said. So, once again it is a balancing act to be able to treat electronic health records as business records, so that they may be admitted into evidence to help your case, on the one hand, while not disclosing personal medical information unrelated to the case which could violate HIPAA regulations, on the other hand.

### Medical Legal Issues Concerning Altering Electronic Records

As most physicians know (at least those who have ever been involved in litigation) even the most innocent changes to a paper medical record, if not executed properly, raise suspicions of a cover up. In the case of electronic health records, any alteration will be time and date stamped, including the identity of who has made the alteration. Cover ups are difficult, at best.

This practice may also apply to patients. Several federal and many state laws give patients the right to view and amend their health records, without regard to the media in which they are kept. Some issues arising from this may be: Will patients be granted special one time access to their online records to view them? Can patients make entries directly into their records? Are patients’ addenda or annotations integrated into the record adjacent to relevant clinician entries? All of these potential actions by patients may have medical legal implications should this record ever be discovered in the course of litigation.

---

## **Safeguards to Avoid and/or Defend Against the Pitfalls**

### Creating and Using the Legal Electronic Health Record (EHR) in Ways to Minimize Medical Legal Risk

For risk management purposes, it is important that there be policies in place that support the EHR as the legal health record. The standards setting organization, HL7, issued the following statement on June 19, 2007 for a 30 day public comment period and probable balloting later in the year: "Because legal validity is at stake for all uses of electronic records as admissible business records, including admissibility as medical records, the legal EHR is of primary importance to healthcare operations and to interoperability."

"When drafting policies and procedures for the EHR, some areas need special attention if the electronic record is to be defined as the legal health record for a patient... For example, cutting, copying and pasting may be efficient for the clinician, but there are risks associated with it. The note may go into the wrong patient's chart. If another person composed the original entry, the original author may object to having her written material used without knowledge or permission. Before organizations create a policy on cutting, copying and pasting, they should investigate limitations of the technology to ensure software compatibility and avoid the production of unreadable notes." *Quinsey, CA, Policies and Procedures for a Legal EHR; Journal of AHIMA; 78(4):62-63 (April, 2007)*

Similarly, organizations' policies should detail how digital photographs and videotapes concerning a patients' condition are to be stored for safekeeping or disclosed. In addition, all verbal orders will be accurately time and date stamped,

making it clear when according to federal and state laws and accreditation requirements, they need to be signed. Finally, there must be policies for physicians to electronically acknowledge their review of test results which guide their clinical decisions (see immediately below). *Cf. generally Quinsey at 62-3*

### Documenting the Information Considered and Justifying the Care Provided or not Provided

The natural downside of having access electronically to more information about the patient and how to diagnose and treat most effectively his or her condition is that it may create greater expectations that physicians use that information. According to Dr. Peter Basch, director of e-health for MedStar Health, a healthcare system in the Washington, D.C. area: "Some physicians are under the mistaken impression that they can read online reports from other providers and not file them in their own EHR, or that they can simply ignore online data. Neither course of action will protect them in malpractice suits, he says, because audit trails will show that electronic messages were sent and/or opened, and a plaintiff's attorney could prove that a physician had access to information but didn't review it."

Jud DeLoss, a healthcare and medical defense attorney with Krahmer and Nielsen in Fairmont, MN agrees: Not reviewing that information and then doing something involving incorrect treatment or prescribing would be a violation of the standard of care." *Terry, K, Will an EHR affect your Malpractice Risk? at: <http://www.memag.com/memag/article/articleDetail.jsp?id=438102>*

According to Marilyn Lamar, Esq., a leading health care IT attorney, to minimize this risk, physicians must be able to use electronic systems that:

- Permit them to document their rationale for not taking into account certain available online data (from outside their own practice and patient population database) about the patient or concerning the diagnosis or treatment of his or her condition which could alter their current clinical decision making;
- Provide “prompts” to physicians to discuss certain information about their health and current clinical conditions with them during each visit; and
- Remind them to periodically review the clinical alerts within their electronic systems to readjust them, if necessary, so that there is not built up a substantial, discoverable electronic record documenting the ignoring of these alerts intended to aid clinical decision making.

Physicians need to know how to use their electronic systems as a justifiable shield against unwarranted medical liability claims. They need to document their clinical rationale for not following alerts or tamping down their sensitivity. Electronic health records must have required prompts for physicians to justify clinically their overriding of alerts or practice guidelines.

Physicians also need to be able to use the graphics capabilities of electronic health records illustrating patient care results to document the effectiveness of the care provided and justify the subsequent clinical decisions made or not made. All of these features need to be available in electronic health records. However, it is still up to each individual physician to put these features to best use in patient care.

## Strict Adherence with all of the CCHIT Privacy and Security Criteria

Violations of the privacy of personally identifiable patient information or medical identity theft have been paramount concerns in the drafting of the CCHIT criteria for both ambulatory and inpatient electronic health records. Consequently, any EHR system to be CCHIT Certified according to the latest criteria must fulfill stringent requirements to ensure the security of electronic health records from unauthorized disclosure or other violations of medical privacy. To be CCHIT Certified, everyone who accesses the electronic health record must be recorded.

While it may be important to establish electronic health records as business records for legal purposes, (see above discussion on the Legal EHR), it is equally important that personally identifiable medical information be protected. In addition to the strict security requirements protecting all aspects of electronic health records from unwarranted disclosures, to be CCHIT Certified, electronic health records must provide added precautions to ensure that personally identifiable medical information is not leaked to unauthorized users.

## Prevention of the Alteration of Electronic Health Records without Documentation of the Clinical Rationale

According to CCHIT Chairman, Mark Leavitt, M.D., “the current CCHIT criteria already include certain elements of a legal record, including a requirement that systems have the capability to prepare an audit of who has accessed the medical record and the ability to ‘lock’ the record once it is created, not allowing an alteration of the record without leaving a record of the alteration.”

This feature of CCHIT Certified EHRs should provide a degree of protection to physicians who need to append information to a medical record to justify a clinical course of action subsequently taken. This feature may provide a more defensible record

---

## **Summary Conclusions and Recommendations**

CCHIT Certified electronic health records can provide a myriad of risk management benefits to physicians. However, not even the best CCHIT Certified electronic health records and other safety enhancing technologies are sufficient, in and of themselves, to ensure the delivery of high quality, safe care to patients, while protecting its physician users from litigation. What is still most important is how physicians implement and ultimately use these technologies. More specifically, it is crucial that physicians and other caregiver users understand the safety and risk management benefits of these systems, *when fully and properly used*.

Conversely, they must also appreciate the potential risks involved in not using CCHIT Certified technologies in the intended manner (e.g. by turning off clinical alerts and reminders and other decision support systems). If required, such systems should be adjusted to prevent them from unduly disrupting clinical decision making due to false alarms—but they should not be deactivated, or otherwise ignored.

Proper use of the complete range of safety enhancing features of CCHIT Certified electronic health records will result in improved clinical effectiveness and efficiency. A happy byproduct of these benefits should also be fewer lawsuits, or, at least the ability to defend better those which might still occur.

We are entering in the next 10 to 20 years one of the most dynamic, yet tumultuous, periods of the past century or so in health care. With all due caveats, this multi-trillion dollar industry will move from what is still a predominantly paper based system to an electronic one during this time period.

For there to be high quality, safe, advanced healthcare available for those who need it during this period and beyond, this transition is both necessary and inevitable. Those who have committed their professional lives to the noble service of caring for patients must regard the daily, proper use of electronic information technologies as indispensable to practicing high quality medicine as are their stethoscopes and microscopes. CCHIT is privileged to provide guidelines to ensure the optimal design and use of these critical new electronic technologies.

---

*Disclaimer: This white paper is based on the author's knowledge and experience, the views of the individuals interviewed, and the Certification Commission's 2007 certification program requirements. It should not be construed as offering legal advice. The Commission's certification requirements are evolving, expanding in scope and improving rapidly. Physicians considering buying certified EHRs should exercise their own due diligence in validating a selected certified product's configuration against their own unique medical and legal requirements and circumstances.*

## About the Author

James B. Couch, M.D., J.D., FACPE is the Managing Partner & Chief Medical Officer of Patient Safety Solutions, LLC, a company dedicated to evaluating and improving safety culture, systems and technologies in all types of healthcare organizations. Over the past 30 years as a practicing physician, attorney and senior executive for several health care, financial, legal and professional services organizations, Dr. Couch has devoted his career to healthcare quality and patient safety, especially where the practice and principles of medicine, law, information technology, business and risk management merge.

For the past 15 months, he served as the chief patient safety consultant to Princeton Insurance Company, the leading liability carrier for physicians and hospitals in New Jersey. He recently served as the lead consultant assisting a \$30 billion company to become one of four successful federal contractors chosen to design the National Health Information Network (NHIN). Dr. Couch also designed and led an unprecedented controlled clinical trial at a major university demonstrating the 707% ROI of a leading clinical decision support system, which trial was published in 2005 in a prestigious peer reviewed journal.

Dr. Couch sat on the AMA House of Delegates (HOD) for four years. He held leadership positions in three national medical specialty societies in the AMA HOD dedicated to improving quality of care. He is the author of three major books on healthcare quality, disease and health management. In 1987, he was the first to publish a fully developed model of medical care value purchasing, now known as "Pay for Performance." He was the first physician to apply Six Sigma process improvement methods to healthcare in 1992. During his three year tenure in the early 1990s as the only physician Senior Examiner for the Baldrige Award, he helped in the early development of that award for healthcare. .

Dr. Couch has lectured on healthcare quality improvement, patient safety, risk management, disease and health management, value based purchasing, information technology, medical predictive modeling and health policy at the University of Pennsylvania's School of Medicine, Wharton Graduate School and Center for Biomedical Ethics, Johns Hopkins School of Public Health, NYU's Wagner School of Public Service and Stern Graduate Business School, Cornell Medical School, Harvard, Yale and Oxford (Green and Wolfson Colleges). He is a Fellow of the Benjamin Franklin Society of the University of Pennsylvania.

Dr. Couch may be reached at:

JCouch9132@aol.com  
(908) 642-6224

## About the Certification Commission

The Certification Commission for Healthcare Information Technology is an independent, nonprofit organization that has been officially named by the federal government as a "recognized certification body" for health information technology products and networks. Its mission is to accelerate the adoption of health information technology by creating a credible, sustainable certification program. The certification requirements are based on widely accepted industry standards and involve the work of hundreds of expert volunteers and input from a variety of stakeholders throughout the health care industry. More information on the Commission and CCHIT Certified products is available at [www.cchit.org](http://www.cchit.org).

"CCHIT<sup>SM</sup>" and "CCHIT Certified<sup>SM</sup>" are service marks of the Certification Commission for Healthcare Information Technology.