Incorporating Technology Into Your Practice

A Guide to Service and License Agreements

Authors

Hal S. Katz, JD • Ana E. Cowan, JD
Brown McCarroll, LLP

TMA gratefully acknowledges the Texas Medical Association Special Funds Foundation for its support of this publication through funds awarded by the Physicians' Foundation for Health Systems Excellence.

Table of Contents

Before You Sign on the Dotted Line

Why Incorporate Technology?

Most physician practices are computerized in some fashion, ranging from simple billing functions and patient scheduling to electronic medical records (EMRs) and entire practice management systems. The benefits of using health information technology (HIT) in health care can be significant. Innovations like EMRs, computerized drug order entry, and clinical decision support systems can increase access to care, decrease the risk of errors, and help improve medical practice efficiency.

The increased use of technology in today's practices is driven by three main factors: 1) patient expectations, 2) government regulatory pressure, and 3) lower costs. Patients want the power to participate in and lead their own medical care. They use the Internet to access information on injuries, prescription drugs, health insurance, and child development. Many make informed decisions regarding their health care based on the information they find on the Web.

Government pressure stems largely from a law requiring that physicians submit Medicare health care claims electronically. Since Oct. 16, 2003, physicians who fail to submit electronic claims risk denial of payment. In addition, the Bush administration has proposed a plan for most Americans to have an EMR within the next 10 years.

Similarly, state regulators are relying on technology to improve patient care and reduce health care costs. State governments offer various programs, grants, or loans to develop statewide networks for electronic medical records.

Finally, the benefits of using HIT in health care include lowered administrative costs and increased reimbursement accuracy. Technical innovations can increase practice efficiency by:

- Integrating clinical records to make them portable and reduce the need for duplicate testing;
- Minimizing errors based on confusion among similarly named drugs, illegible handwriting, incorrect dosage, or unclear instructions;
- Increasing revenue for physician practices due to better documentation;
- Decreasing patient costs for prescriptions because physicians have greater access to formularies; and
- Improving prescription safety because physicians have greater access to contraindication information and patient allergies.

Despite the above advantages, however, a practice must carefully analyze its needs before selecting technology tools to make sure they meet the specific needs of the practice.

Choosing a Specific Type of Service

Deciding to adopt a particular type of technology can be one of the most important decisions a practice makes. The transition to an EMR from a paper system affects the fundamental way a practice is run and the staff's daily schedule.

At a minimum, EMRs can change current documentation methods, workflow, billing practices, scheduling, and patient follow-up methods. Considering the vast changes that have to occur as you adopt various forms of technology — and the possible benefits — you must plan extensively for successful implementation.

Follow these seven steps to determine what type of technology best suits your practice.

Step 1 — Conduct a needs assessment. Determine how health information technology fits into your long-range plans. This requires an analysis of how certain technologies might help your practice, then setting goals that identify and quantify the expectations. For example, the practice might wish to increase physician productivity or strengthen management with the use of specific data and measurement tools. It may want to improve medication management for patients. Or, it may wish to enhance relationships with patients through patient/physician communication software.

Before purchasing any new technology, you should conduct a review your practice's current technology systems to determine if you are using them effectively. You may discover that the practice's current systems will meet its needs if used properly.

Step 2 — Conduct research. The next step is to research the types of technology that will best meet the needs identified during the needs assessment. As a starting point, visit the many Web sites that address various aspects of health information technology. As part of your research process, attend seminars and talk with your peers to obtain valuable feedback

Step 3 — Develop a request for proposal (RFP). Now you can identify several potential vendors, which might include resellers, equipment manufacturers, and software or hardware developers. The practice should develop an RFP that outlines the goals it wishes to achieve through health information technology. In the RFP, ask vendors to provide pricing in as specific a manner as possible, allowing for an "apples-to-apples" comparison of hardware and software costs, as well as implementation, integration, support, training, and maintenance expenses. Additionally, request that vendors supply information regarding the history of their organization, their financial stability, technology partnerships, and, if available, customer references.

Step 4 — Conduct an ROI analysis. It is important to quantify return on investment (ROI) for the practice's specific circumstances. This analysis should identify how the technology system will impact the entire practice, not just one area. If, for example, the system reduces costs in one area of the practice but increases costs in another, you must weigh this trade-off carefully. Part of the analysis should include whether the practice can leverage existing technologies by integrating the proposed technology.

Step 5 — Set up vendor demonstrations. After narrowing down the list to three or four vendors, invite them to give demonstrations, with both physicians and staff participating. Prepare a checklist for rating each system in key areas such as user friendliness, and ask each participant to rate each vendor using this checklist.

Step 6 — Check referrals. Visit other practices that have used each system that you are considering seriously. Include practices that are not on the vendor's official reference list.

Step 7 — Negotiate the best deal possible. Generally, the first offer made by a vendor is not its bottom line. Too often, practices fail to negotiate, even though the result can be "win-win" for both the practice and the vendor.

By following these seven steps, your practice can be certain that the investment it makes will pay off. Remember also that technology is constantly changing, so ongoing assessments of the practice's needs essential. Stay abreast of HIT advances just as you always have done with patient care.

Legal Issues to Consider

Along with the host of possible benefits, the use of technology presents a complicated web of legal issues. Below is an overview of relevant issues and practical consequences that you should consider before implementing any type of technology.

Antikickback and Stark Rules

Among the primary legal barriers are the antikickback statutes and the Stark antireferral rules. Antikickback laws are implicated when a practice or physician gives something of value for referrals. Stark issues arise when a physician refers to an entity with which he or she has a financial relationship. Despite the serious limitations these regulations impose, regulators have taken action to help protect certain types of arrangements involving electronic media.

E-prescribing. Electronic prescribing presents various advantages to both physicians and patients, ranging from efficiency and convenience to fewer clinical errors. Unfortunately, most physicians cannot afford to develop this type of technology without the support of a hospital or third party. For this reason, the U.S. Office of the Inspector General (OIG) recently proposed a new safe harbor to foster e-prescribing. A parallel exception has been proposed under Stark as well.

Any physician considering entering into an e-prescribing relationship with a third party should be aware of these restrictions:

- The only services a third party may provide the physician are hardware, software, and training needed solely to send and receive electronic prescription drug information.
- Only the following may provide items and services: 1) a hospital to physicians who are members of its medical staff; 2) a group practice to physicians who are members of the group; or 3) a Prescription Drug Plan (PDP) sponsor or Medicare Advantage (MA) plan that offers drug coverage.
- The items or services donated must be part of or used to access an electronic prescription drug program that meets the applicable standards under Medicare Part D at the time the items are furnished.
- There can be no restrictions on the use of other systems.
- It is not proper to take into account the volume or value of referrals or other business generated between the parties.
- The parties must sign a written agreement that: 1) specifies the items or services being provided and their value; 2) covers all of the e-prescribing services to be furnished by the entity; and 3) contains a certification by the physician that the items and services are not technically or functionally equivalent to items and services that he or she already possesses or has obtained.

Because safe harbors for e-prescribing comprise a new area of regulations, you always should find out if government regulators have issued additional guidance before entering into these type of arrangements.

From the TMA Code of Ethics

Patients have the right to have a prescription filled wherever they wish and physicians should respect the patient's freedom of choice. The use of e-prescribing programs that require prescriptions be dispensed from a particular pharmacy while also refusing to provide a paper prescription to permit the patient to choose where to fill the prescription is unethical. Further, physicians should avoid situations which inappropriately limit the patient's medication options.

EMRs. There is a new proposed exception to Stark for electronic medical records that would protect nonabusive arrangements under which third parties provide medical practices the software and training they need to receive, transmit, and maintain EMRs. The comment period is currently open for this exception.

Restrictions related to EMRs include:

- The only services that a third party may provide the practice are the software and training needed solely for the transmission, receipt, and maintenance of EMRs. The items and services cannot include any billing, scheduling, or other similar general office management or administrative software or services, or staffing of physician offices.
- Only the following may provide items and services: 1) a hospital to physicians who are members of its medical staff; 2) a group practice to physicians who are members of the group; or 3) a PDP sponsor or MA organization to prescribing physicians.
- There can be no restrictions on the use of other systems.
- It is not proper to take into account the volume or value of referrals or other business generated between the parties.
- The parties must sign a written agreement that: 1) specifies the items or services being provided and their value, 2) covers all of the EMR items and services to be furnished by the entity, and 3) contains a certification by the physician that the items and services are not technically or functionally equivalent to items and services he or she already possesses or has obtained.

- The EMR technology must contain e-prescribing capabilities that comply with the electronic prescription drug standards under Medicare Part D at the time the items and services are furnished.

As with e-prescribing, be sure to find out if government regulators have issued additional guidance before pursuing this type of arrangement.

Liability Exposure

Various forms of technology may carry different types of risk requiring different types of liability insurance coverage. For example, if your practice management system does not properly back up files and a patient's record is lost, does your general liability insurance cover any resulting claim? What if the integrity of an e-prescription is compromised upon transmittal and dosages are changed?

Technology is not simply an instrument to increase practice efficiency; it comes with the added responsibility of ensuring the technology works properly. With the increased prevalence of technology, physicians may be subject to a higher standard of care than before.

You should accommodate this added responsibility when negotiating contracts and purchase the practice's insurance coverage. Consider these factors:

- You will need a general liability policy (not a medical liability policy) to cover equipment malfunctions, data transmission errors, incomplete or inaccurate data resulting in inaccurate medical diagnoses, misappropriation of confidential health care information, and other related issues.

- Physicians using the Internet or an EMR as part of providing medical services should determine whether their medical liability policy covers services provided electronically.

- Most medical liability insurance covers only "face-to-face" encounters within the state in which the physician practices and is licensed. Consequently, physicians who provide services over the Internet or telemedicine services to patients outside the state can be exposed to claims if state law requires the physician to be licensed in the state where the test results are delivered.

Be sure to always obtain written assurances from vendors that they are responsible for claims that may arise as a result of a defect or malfunction of their products. See the Contract Review Checklist for details on obtaining representations.

HIPAA

By now, all of the health care industry has heard of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA requires physicians to protect the confidentiality and integrity of patient information.

HIPAA policies and procedures are extensive and complicated, and the majority of physician offices simply do not have the technical expertise needed to comply with the regulations. For this reason, practices should obtain written assurances from their technology vendors that they comply with HIPAA and will remain so throughout the term of any agreement. Ask your vendor these questions:

- Does it give physicians the ability to document their compliance with HIPAA?

- Does it notify the physician of authorizations that have been revoked or expired?

Note that with the adoption of any new technology, the practice may need to reissue its Notice of Privacy Practices (NPP) and obtain updated authorizations. The NPP should disclose whether the physician e-prescribes or communicates with patients via e-mail.

Telemedicine

Many physicians engage in telemedicine without realizing it. Telemedicine consists of a health care service that a physician initiates for purposes of assessment by a health professional, diagnosis or consultation by a physician, treatment, or the transfer of medical data, and that requires the use of advanced telecommunications other than telephone or fax.

Historically, telemedicine served as a health care alternative in remote areas, but now it is more common in standard practice as it enables specialists to review a patient's record and/or provide care when a patient seeks care in a different location. Thus a radiologist in Texas can easily examine test results for a patient in Iowa.

When incorporating telemedicine into your practice, you must comply with Texas-specific requirements. For example, a practice must create and follow written protocols that document a good faith effort to prevent fraud and abuse by addressing the following:

- Authentication and authorization of users;
- Authentication of the origin of information;
- Prevention of unauthorized access to information;
- System security, including the integrity of information collected, the program, and the system;
- Information storage, maintenance, and transmission;
- System and information usage; and
- Synchronization and verification of patient data.

The Internet

The Internet enables physicians to deliver health care in a more efficient and cost-effective manner. Note that Texas law holds online treatment and consultation recommendations, including e-prescriptions, to the same standards as traditional (face-to-face) settings.

An online or telephonic evaluation by questionnaire will not constitute an acceptable standard of care. As a result, Texas physicians who use the Internet for patient care must first establish a proper patient-physician relationship, which includes at a minimum:

- Establishing that a person requesting treatment is in fact who the person claims to be;
- Using acceptable medical practices such as patient history, mental status, physical examination, and appropriate diagnostic and laboratory testing to establish, diagnose, and identify underlying conditions and/or contraindications to treatment;
- Discussing with the patient the diagnosis and evidence for diagnosis, and the risks and benefits of various treatment options; and
- Ensuring physician availability and/or coverage for appropriate follow-up care.

Web Sites

Web sites traditionally have been used as a means of marketing. However, more and more physicians are creating Web sites as a means of providing treatment and directly communicating with patients. The use of Web sites triggers both federal and state regulations, including many of the legal aspects previously discussed. In addition, Texas law requires any physician establishing a Web site to disclose clearly:

- Ownership of the Web site;
- Specific services provided;
- Office address and contact information;
- Licensure and qualifications of physician(s) and associated health care providers;
- Fees for online consultations and methods of payment;
- Financial interest in any information, products, or services offered;
- Appropriate uses and limitations of the site, including providing health advice and emergency health situations;
- Uses and response time for e-mails, electronic messages, and other communications transmitted via the site;
- To whom patient health information may be disclosed and for what purpose;
- Rights of patients with respect to patient health information;
- Information collected through any passive tracking mechanism; and
- A liability disclaimer

Electronic Communications

Physicians who communicate with patients through e-mail or other communication software should implement policies and procedures addressing the proper scope for such communications. Under Texas law, practices should periodically evaluate communication policies for compliance with current regulations and address the following:

- Privacy mechanisms to assure confidentiality and integrity of patient-identifiable information;
- Hours of operation and availability;
- Which health care personnel, in addition to the physician, are authorized to process messages;
- Types of transactions that are permitted electronically;
- The type of required patient information that may be included in each communication, such as patient name, identification number, privacy statement, and type of transaction;
- Means of archival and retrieval; and
- Quality of oversight mechanisms.

Patients should sign an authorization accepting the use of e-mail and/or other forms of patient-physician communication programs. The authorization should explain the inherent risks of disclosure associated with this means of communication and inform patients of alternative forms of communication for urgent matters. Physicians engaging in this type of communication should store and file all communications in the patient's medical record.

Internet Prescribing

In today's high-tech environment, physicians are linking to clinical databases, formulary systems, and electronic care management systems to deliver care. Some team up with online pharmacies and prescribe medications to patients over the Internet and across state lines. As with any new technology-based practice, prescribing drugs online presents certain legal and ethical challenges for physicians, including:

Texas Medical Association
Guidelines for Electronic Communications

- Establish turnaround time for messages and exercise caution when using e-mail for urgent matters.
- Inform patients about privacy issues such as:
  - Who will processes messages during usual business hours and vacation or illness;
  - The level of security of the communication system used; and
  - That the message will be included as part of the medical record, at the discretion of the physician.
- Establish types of transactions (prescription refill, appointment scheduling, etc.) and sensitivity of subject matter (HIV, mental health, etc.) permitted over e-mail.
- Instruct patients to put the category of the transaction in the subject line of the message for filtering: prescription, appointment, medical advice, billing.
- Request that patients put their name and patient identification number in the body of the message.
- Configure automatic reply to acknowledge receipt of messages, and send a new message to inform patient of completion of request.
- Print all messages, with replies and confirmation of receipt, and place in patient's paper chart.
- Request patients to use an auto reply feature to acknowledge reading clinician's message.
- Develop archival and retrieval mechanisms.
- Maintain a mailing list of patients, but do not send group mailings where recipients' names or addresses are visible to each other.
- Avoid anger, sarcasm, harsh criticism and libelous references to third parties in messages.

Licensure. Generally, states require that a physician be licensed in the state in which he or she practices. Unfortunately, there is not much consistency among the states. Some states require a physician to obtain a license in each state where the physician provides services, while others issue special licenses to out-of-state physicians. Similarly, online pharmacies also are required to be licensed in the jurisdictions in which they operate.

Standard of care and liability. The risk of medical liability may be greater with Internet prescribing. The Federation of State Medical Boards policy on Internet prescribing says that a physician who prescribes medications based solely on an electronic medical questionnaire clearly fails to meet an acceptable standard of medical care. Although the patient-physician relationship is not always precisely defined in an online setting, it is clearly established upon the diagnosis and treatment of a patient, which typically occurs after the patient completes an online questionnaire and the physician communicates with and prescribes medication to the patient.

Informed consent. Requiring informed consent for certain medical procedures such as surgery is a well-established legal doctrine. Given the risk of liability for unauthorized disclosure, invasion of privacy, and breach of confidentiality inherent in prescribing medication online, physicians should take certain precautionary measures, including obtaining the voluntary informed consent of the patient for Internet prescribing. This consent should be documented in a written agreement between the parties, signed by the patient, and included in the medical record. Once the patient has been advised of the risks and benefits, he or she can make an informed decision as to whether or not to accept Internet prescriptions.

Patient confidentiality. Physicians have long had an ethical and legal duty to protect the confidentiality of patient communications and information. This standard applies irrespective of the form in which the confidential information is transmitted.

In addition, the American Medical Association recommends that physicians who prescribe medication online adopt the following additional safeguards:

- Engage in adequate dialogue with patients about treatment options, risks, and benefits;
- Follow up with patients as necessary and appropriate;
- Maintain an updated medical record that is readily available to the patient as well as other health care professionals (upon patient consent);
- Include the electronic prescription information in the patient's medical record; and
- Clearly disclose physician-identifying information on the Internet, including the physician's name and practice address and any financial interest he or she may have in any of the products prescribed.

Although the above guidelines do not necessarily eliminate a physician's potential liability, they clearly provide a base for compliance to an "industry guideline." Any practice endeavoring to engage in Internet prescribing should formulate clear policies and procedures implementing the AMA guidelines and provide regular training to staff.

From the TMA Code of Ethics

Although the development of telecommunications technology now makes it possible for physicians to prescribe medications by means of the Internet, such prescription writing may be unethical.

The medium of the Internet itself imposes limitations on communications that are not present in a traditional office setting, or even in a telephone conversation. However, there may be situations in which Internet prescribing may be appropriate, e.g., when a prior long-standing physician-patient relationship exists between the physician or other physicians and the individual requesting the prescription or in emergency or short-term situations.

If the individual seeking a prescription, has never been a patient of the physician, it is not ethically appropriate for the physician routinely to prescribe the requested medication without the benefit of a hands-on examination.

The User-Friendliness Factor

While the vendor contract itself is extremely important (and you should have a competent advisor evaluate it carefully before you sign), it is up to you to discover how "physician-friendly" or "patient-friendly" the contract really is. Below is a list of questions to ask the vendor sales representative.

Vendor Responsiveness

- Will I have a dedicated representative who will know my office and its needs and how often can I expect to see him or her?
- How easily can I reach my representative if I have a question or a problem?
- Do you provide initial and refresher training?

Initial Issues

- Does my practice or medical group need special software to use the vendor services?
- What data are migrated from our old system?
- Do I have the appropriate infrastructure? Is additional hardware necessary?
- Does the system support, in a fully integrated fashion, patient scheduling and recalls?
- How are patients registered on the system? Can patients be registered in "bulk"?
- Is it possible to track patients?
- What kind of clinical documentation is in place?
- Does the program support a document management system?
- What kind of coding and compliance procedures are in place?
- Can the system capture charges, claims, and remittance information?
- How are correspondence and phone calls documented?

Scheduling and Patient Information

- Can the program be used at multiple locations and by multiple resources?
- Is it possible to implement practice-specific scheduling templates?
- Does the system provide the ability to copy data entered in a preceding registration (e.g., guarantor information for two children)?
- Is it possible to merge two master patient account records for the same person (e.g., duplicates, erroneous registrations)?

Authorization and Referrals

- How are authorizations documented and tracked?
- Is it possible to track authorizations and referrals by status?
- Are there automatic alerts if an authorization is no longer applicable or revoked?

Documentation

- Can patient-relevant documents and images be attached to the corresponding areas of the EMR?
- Can old charts be scanned and integrated into the system?
- Is there an automatic aggregation of documents and images by specific areas of the patient record (imaging, referrals, Rx, or lab)?
- Is it possible to store and view documents and images in different formats?
- Is it possible to provide in a single view the progress of all clinical elements in time, related to a condition?

Order Entry

- Does the system have an electronic prescription writer with a complete drug database?
- Is there automatic drug reaction checking for all clinical information on the chart (drugs, conditions, symptoms, pregnancy, lactation)?
- Is it possible to transmit and fax prescriptions?
- Does the system provide a Medicare compliance-checking feature for medical necessity?

Coding and Billing

- To what extent can the system communicate with different providers and clearinghouses?
- What kind of reports can be generated?
- Does the system provide code sequencing and code optimization features?
- Is there an automatic evaluation and management coding engine integrated with clinical documentation?
- Are there prompts for missing data elements required for certain visit levels?
- Does the system provide the framework for coding justification for any possible audits?
- Can there be separate fee schedules set up by physician/clinic?
- In relation to insurance updates, is it possible to retrieve an expired plan and update it so that it can be active again? Would it maintain the integrity of the insurance as it was originally entered?
- Does the system track member yearly and lifetime benefit limits by procedure and warn users when utilized benefits approach or exceed limits?

Communication With Data Exchange

- Does it interfere with our current clearinghouse and payers? Is it difficult to add or change clearinghouses or payers?
- Is it possible to communicate with labs and other diagnostic facilities?
- Can patient charts be exported and imported?

Security

- Does the system incorporate all HIPAA compliance security features?
- Is it possible to filter views according to user rights?
- What strategies are in place for recovering records?
- Are procedures in place that create and maintain retrievable exact copies of EMRs?

These are some of the questions you should ask before signing a contract with a vendor. Certainly, there are many more areas you might consider, and the contract should specifically address the practice's expectations.

Do not hesitate to ask for physician references, and do call and talk with doctors and front office staff who have worked with the vendor. Be sure to contact the Texas Medical Association or your county medical society for any additional information they may have on any vendors you are considering.

Careful investigation can help you find the plan that will be best for your practice.

Contract Review Checklist

After taking the time to research vendors and set up demonstrations, you will want to ensure that the selected vendor delivers its promised services. For this reason, a written contract that clearly meets the practice's needs, goals, and security expectations is crucial.

The specificity of vendor contracts varies — in part, with respect to the size and technical capabilities of a practice. For example, many larger practices and clinics hire IT personnel to oversee the security of data and create individualized software interfaces unique to their practice. In these situations, specific interface provisions that will maintain the integrity of existing programs may be necessary.

A smaller practice, on the other hand, may be completely reliant upon the contracted vendor for all of its security, software, and integrity needs. In such a case, the vendor's capabilities become particularly relevant, and the practice will want to ensure that the vendor's program not only meets its specific needs but also facilitates compliance with federal and state law. At a minimum, all vendor contracts should address the following factors.

❑ 1. **New contract or renegotiation?**
Is the proposed contract arrangement a renegotiation with an existing vendor or new relationship? While everything discussed below applies equally to negotiations with existing vendors, physicians should view renegotiations as an opportunity to evaluate the vendor's performance and make needed changes.

❑ 2. **Contract term.**
The contract should clearly state 1) the beginning or effective date and 2) the ending or expiration date.

❑ 3. **Contract parties.**
The contract should include the full name, address, legal status (e.g., corporation, partnership), and contact person of the other party. Verify that the vendor identified in the contract is the party that it has been dealing with, and not a less solvent subsidiary or affiliate. Finally, pay close attention to the definition of a "licensee." You may want to widen the scope of licensed parties to include use by affiliates or related parties.

❑ 4. **Duties and obligations.**
The contract should clearly state all duties and obligations of the practice and the other parties to the contract so that all know: 1) what the duties and obligations of each party are, 2) how each party is to perform them, and 3) when they will perform them. The contract should be evenhanded so that both parties are subject to similar obligations.

❑ 5. **What is being licensed and its purpose.**
Contracts frequently fail to identify exactly what is licensed and the functions performed. An exhibit outlining functions that the software performs is the ideal way to include this information — the more detailed, the better for the practice. You may also consider creating an exhibit with an understanding of what the licensed program will do (e.g., the specifications). If nothing else, consider attaching brochures, presentations, or any other document the vendor provided. Some questions to ask your vendor are:

- In which format is the software is delivered?
- What type of user documentation is required?
- Will use of the software require purchase of hardware owned by third party? If so, how much will it cost?
- Are updates included in the license agreement?
- Will the version that the practice is licensing be phased out over the next two years and no longer be supported?

❑ 6. **Scope of license.**
The contract also should specify the scope of the purchased service. For example, a contract may be "exclusive" or "nonexclusive." The issue of exclusivity may not be important if the practice uses mass-produced or retail software; however, it becomes very important if the practice pays a programmer to develop custom software.

In addition, a vendor contract may refer to the "use" of the software. As a licensee, the practice should seek a broad license that will not limit future use if the practice later expands.

In addition to limiting the scope of the license to internal use only, vendors commonly attempt to limit:

- Number of users,
- Right to create derivative works,
- Territory and industries covered,
- Who can perform repairs (i.e., only the licensor),
- Use as a service bureau,
- Right to sublicense, and
- Location (if the practice has facilities in nearby towns or cities that will need to use the software, you don't want a license that is limited to a particular location or facility),

Finally, the contract should stipulate if the license is transferable or nontransferable. A physician who sells his or her practice will want the license to be transferable to the buyer, or else the buyer will have to get a new license to use the software (and the buyer may seek to lower the purchase price for the practice).

❑ 7. **Compliance with laws and standards**.
The vendor should agree to comply to applicable laws and any applicable accreditation standards.

❑ 8. **Payment and fees.**
The contract should clearly and accurately state the amounts the practice is obligated to pay under the contract, and clearly establish place, time, and method of payment following receipt of an agreed-upon invoice. Payment methods vary greatly and may include flat monthly rates, amounts based on usage time, or fee schedules based on the number of system users or the quantity of data hosted. Consider the following when evaluating the contract for payment information:

- If the payment schedule calls for a down payment, the contract should make clear as to whether there are also additional annual payments.

- If the payment schedule calls for a down payment plus royalty, the contract should clearly outline how the royalty is calculated and what is deducted.

- Consider incorporating provisions that allow for a right to change or modify pricing within a certain range after one or two years. Alternatively, the practice may prefer a right to change pricing after the initial term.

- The contract should outline whether support services are provided as part of the fee or whether the fee includes any customization services.

- The contract should outline whether training services are included in the initial payment fee. If so, the contract should clarify who will provide the training and to what extent — and whether the training will be "live" or through "remote services."

Ideally, the physician and vendor should anticipate changes in the volume of system users and data requirements when agreeing to initial terms.

❑ 9. **Privacy and security.**
The contract should require the vendor to maintain and document a comprehensive privacy and security program that includes administrative, technical, and physical safeguards to reasonably and appropriately protect the confidentiality, integrity, and availability of electronic health information as required by HIPAA. The contract should require the vendor to provide documentation upon the practice's request.

❑ 10. **Disclosure protocol.**
The vendor should have an established protocol for reporting to the practice any inappropriate disclosures of information that may occur.

❑ 11. **Termination.**
A contract may set forth various types of termination provisions, including:

- A fixed, initial term with automatic renewal thereafter (termination 30 days prior to renewal);

- A fixed term with annual renewal unless terminated with prior notice;

- Termination for physician's convenience (this gives the practice the most freedom to get out of the license); or

- A provision allowing either party to terminate only in the event of material breach.

At a minimum, the physician should be permitted to terminate for the following events:

- Vendor's failure to maintain state licensure or comply with legal requirements imposed upon the practice;
- An increased number of patient complaints or the practice's perception that serious problems in care quality have occurred as a result of the vendor's failure to comply with the agreement;
- Vendor's failure to maintain system performance resulting in system downtime (98 percent performance), compromised data integrity and/or security, or a physician's ability to render services; or
- Vendor's failure to mitigate consequences or implement appropriate safeguards in the event the vendor makes inappropriate disclosures.

❑ 12. **Wind-down provision**.
The practice should attempt to include a wind-down provision to protect it from the effects of termination by a vendor. For example, the vendor should be obligated to cure any material breaches prior to ending the relationship, to cooperate with new service providers or vendors, and especially to migrate or transfer electronic information in a mutually agreed upon format at no additional cost to the physician.

❑ 13. **Data ownership.**
If applicable, the contract should clarify the ownership of data contained in or generated by the system, and designate the practice as the owner of all patient information, confidential information, or any derivative thereof. The contract also should clarify the format in which information is to be returned, the method for returning the information, and the timeframe. This provision should apply equally to subcontractors.

❑ 14. **Software ownership.**
The contract should address who has ownership rights to licensed software and set forth who owns derivative works to the software, whether the practice has the right to modify software, and ownership rights in any modifications. Ownership rights become especially important if the practice initiates and makes modifications to the software.

❑ 15. **System updates and changes.**
The practice should ensure that the vendor provides notice of any updates the vendor issues for compliance with federal or state regulations or to address security or operability issues.

❑ 16. **Testing/quality assurance.**
If the vendor is providing solutions or modifications unique to the practice, the contract should ensure that the vendor tests systems to verify that they will meet the contract requirements. You may request that the vendor provide evidence of having tested systems or system components under simulated conditions similar to those that you contemplate will occur in your practice. This will ensure that the vendor is able to address all of your needs. Because such quality assurance requires a high degree of expertise, the practice and vendor may contract with a third party to review the systems for contractual compliance and identify potential issues.

❑ 17. **Support services.**
The contract should specify whether support is provided by a third party or the vendor. Issues to address include:

- Is there a 24-hour help desk?
- If support is needed at the practice's site, who pays for the travel time and expenses?
- How quickly will the vendor respond to requests for support services?

❑ 18. **Representation and warranties.**
Warranties obtained from a vendor will vary greatly depending on services provided. Evaluate the following:

- Whether the contract includes a "performance warranty" that the software will actually perform the functions the seller claims it will. These functions usually are outlined in a specification sheet, preferably attached to the license agreement.
- Vendors typically try to avoid a performance warranty or include language that leaves them wiggle room, such as: "substantially comply with specifications"; "no known major bugs"; or "free from defects as delivered. Instead, the practice should try to insert contract language that says the software will: "operate in accordance with the specifications"; or "conform to specifications".

- Whether the support services will be performed in a professional or quality manner. Good warranties include this language (in order of preference):
  - "Good and workmanlike manner,"
  - "Timely and professional manner,"
  - "In a commercially reasonable manner," or
  - "In accordance with standards generally observed in this industry for similar software."
- Whether the provided hardware and computer programs constitute all applications, systems software, or interfaces required to operate computer programs.
- Whether computer programs are compatible with the practice's existing data files, business information, and systems, so that significant additional applications, software, or interfaces are not required.
- The amount of time for which the vendor agrees to maintain uptime of services during a calendar month. (Typical usage time is near 98 percent.)
- The vendor's agreement to repair or replace a defect, or alternatively, to provide a refund.
- The vendor's representation that the media in which the computer programs are delivered shall be free of any defect, virus, or other program designed to erase or otherwise harm or collect unauthorized information from the physician's hardware, data, or other programs.
- Whether the vendor ensures that services for which it is responsible are free of defect or malfunction.
- Whether each party has the power and authority to execute, deliver, and perform the obligations under the contract and that the person signing the contract is authorized to perform these functions.
- The physician should be leery of negation of warranties. Disclaimers sought by vendors include:
  - "As is" — all warranties are excluded,
  - "Software contains no known viruses," or
  - Disclaimer of implied warranties under a statute commonly referred to as the Uniform Commercial Code or UCC.

❑ 19. **Liability.**
Licensors typically insist on disclaimers of particular damage remedies. Try to limit the contract so that the vendor is still liable for actual damages caused by the software. The vendor should be liable for any claims directly attributable to product malfunction or failure to protect integrity of information. Also look out for provisions capping any liability at a certain amount (e.g., license fees paid) and whether such provisions apply to indemnificatory obligations.

❑ 20. **Downtime provisions.**
In any data-hosting arrangement, there will be times when access is unavailable because of periodic maintenance procedures or repairs. The vendor should agree that any controlled downtime will occur only on an "as needed basis" and not exceed three hours per week. The vendor should give the practice at least 48 hours prior written notice of controlled downtime and use its best efforts to schedule the downtime during nonbusiness hours.

❑ 21. **Subcontractors.**
If a vendor subcontracts work, the subcontractor or agent must be held to the same standards for protecting the confidentiality and integrity of patient information as the original vendor. Each subcontractor or agent must be subject to Texas jurisdiction and venue — especially in today's environment where a large percentage of work is subcontracted to other countries such as India.

❑ 22. **Personal services.**
If the contract is for personal services (as in many consulting agreements), it must clarify the independent contractor status of the vendor.

❑ 23. **Insurance.**
The contract should specify the amounts and types of insurance that the vendor is required to carry.

❑ 24. **Arbitration.**
Almost all agreements contain a process to arbitrate disputes. Be sure to review these provisions carefully. At a minimum, the arbitration section should stipulate that the arbitrator(s) have expertise in the matter to be arbitrated and that the process be conducted in accordance with the Arbitration Rules of the American Arbitration Association. The contract also should require that any arbitration take place in the city within which you practice.

In addition, decide if your arbitration clause should:

- Designate particular people or positions to be involved in early resolution of disputes;
- Require parties to negotiate in good faith to resolve disputes informally;
- Establish if it is possible to withhold payments over disputed invoices;
- Specify whether all disputes should be resolved by arbitration (you may want use of a courthouse for certain types of claims, such as breach of confidentiality or violation of intellectual property rights);
- Set limits on the authority of arbitrators or scope of relief; or
- Stipulate recovery of attorney's fees and court costs.

❑ 25. **Venue.**
Make sure the contract contains no clauses that make it subject to either the substantive law or the jurisdiction (also referred to as "forum" or "venue") of another state; the contract should reference only Texas.

❑ 26. **Assignment.**
An assignment clause sets forth whether or not you will be allowed to transfer your rights or obligations under a contract to a third party. There are many different types of assignment clauses, such as those under which:

- Either party has assignment rights;
- The vendor may assign but not the physician;
- Neither party may assign without consent of the other party, but consent shall not be unreasonably withheld;
- Neither party may assign, unless the assignment is in connection with transfer of all or substantially all assets of the party; and
- The vendor may retain right to renegotiate terms if assigned by the physician.

Ideally, neither party should be allowed to assign the contract without the prior written approval of the other party.

❑ 27. **Source code escrow.**
As a licensee, it is in your interest to seek a source code escrow under the contact. This ensures that if the vendor goes out of business, a copy of the source code is available so that the practice can continue to use it and have repairs made to it. Items to consider include:

- Escrow location,
- Access terms,
- Payment for upkeep of escrow, and
- Duty to keep updated version of source code in escrow.

❑ 28. **Promised items.**
The contract should expressly incorporate all representations, promises, inducements, and warranties that are made to the practice (i.e., verbal assurances and representations that have material influence in convincing the practice to enter into the contract).

❑ 29. **Integration.**
The practice should obtain and review all documents that relate to the contract or are referred to in the contract, as well as any policies and procedures referenced in the contract.

Meet the Authors

Hal Katz, Partner
Brown McCarrol, LLP

Phone (512) 703-5715
Fax (512) 480-5022
E-mail hkatz@mailbmc.com

Legal Experience

Hal Katz is board certified in health care law by the Texas Board of Legal Specialization. His clients, whom he advises on corporate, transactional, regulatory, and public policy matters, are those doing business within the health care industry, including physicians and hospitals across Texas. Mr. Katz is a regular speaker on issues relating to managed care, business relationships, and health care transactions.

Education

- Doctor of jurisprudence, University of Houston Law Center, 1995
- Bachelor of arts, The University of Texas at Austin, 1992

Professional Licenses

- Attorney at law, Texas, 1995
- Texas Board of Legal Specializations, health care law, board certified

Specific Matters of Representation

- Formation of medical groups in urban and rural areas,
- Representing major hospital districts in the creation of HMOs for participation in Medicaid Managed Care and the Children's Health Insurance Program,
- Formation of large medical group wrap-around IPAs engaged in risk sharing and fee-for-service contracting,
- Reviewing and negotiating risk-sharing agreements between HMO and physicians organizations, and
- Formation of PHOs in urban and rural areas.

Ana E. Cowan, Associate
Brown McCarrol, LLP

Phone (512) 703-5791
Fax (512) 480-5009
E-mail acowan@mailbmc.com

Legal Experience

Ana Cowan represents clients doing business within the health care industry, advising them on transactional and regulatory matters. Her experience includes working with physicians, hospitals, chiropractors, dentists, multispecialty groups, mental health/mental retardation centers, and hospital districts. Ms. Cowan is fluent in Spanish and is a regular speaker on health care issues.

Education

- Masters of law, University of Houston Law Center, 2001
- Doctor of jurisprudence, The University of Texas School of Law, 2000
- Bachelor of science, Trinity University, 1997

Professional Licenses

- Attorney at law, Texas, 2000

Specific Matters of Representation

- Advising clients in the formation, merger, and acquisition of medical groups;
- Interpreting and applying Stark and antikickback statutes to physician arrangements;
- Advising IPAs and PHOs on the application of antitrust laws;
- Advising clients in the formation of individual medical practices and medical groups; and
- Advising clients on the consequences of fee-sharing and other compliance issues such as HIPAA.