Click here to access program session audio.

THE ELECTRONIC MEDICAL RECORD – LESSONS LEARNED

Melissa L. Markey
Lisa Vandecaveye

February 14, 2008

I. Background

The rise of electronic medical records (EHRs) has brought with it the promise of a host of benefits. They are expected to improve patient safety by reducing the rates of medical error and eliminating unnecessary or duplicate procedures. Use of e-prescribing systems capable of tracking medication from receipt at the pharmacy to administration at the bedside are expected to help avoid medication errors. Alerts flag possible mistakes in dosage or drug-drug interactions as soon as orders are entered. Decision support systems can recommend best practices such as vision and kidney function checks for diabetic patients. Where the patient's medical record is available electronically, multiple providers can be given access to it, enhancing communication and potentially avoiding repetition of lab tests or invasive procedures.[1]

Patients have taken an interest in EHRs. A recent consumer found that two-thirds of patients consider an EHR at least slightly important in choosing a physician. Over seventy percent would like to be able to email their physicians and receive reminders via email, and fifty-one percent said that they would be willing to pay a reasonable price for the service. EHRs offer patients the convenience of avoiding endlessly filling out the same information over and over for each caregiver they see. Portable, complete, secure medical records have the potential to greatly benefit patients who see multiple providers and those who suffer from complex, chronic conditions.

Payors also have much to gain from the widespread use of EHRs. The elimination of unnecessary or duplicate procedures means more efficient care and less money changing hands. Electronically maintained records make it easier to prevent and correct both inadvertent billing errors as well as intentional fraud. Increased automation in eligibility and billing transactions reduces costs further.

Even the government thinks that EHRs are a great idea. As will be discussed in the next section, a variety of initiatives have been adopted at both the federal and state levels to incentivize the adoption and standardization of EHRs. These range from sweeping goals such as President George W. Bush's push for most Americans to have electronic records by 2014, to safe harbors from Stark and Anti-Kickback enforcement, to outright gifts of entire systems.

With such broad interest and tremendous anticipated benefits, the question arises: why haven't EHRs been broadly adopted throughout the American medical landscape?

[1] See, e.g., Drake Bennett, *Best practices - Unlike the Army's Walter Reed hospital, the VA hospital system is ranked, by many measures, as the best in the country*, Boston Globe, Mar. 11, 2007, 2007 WLNR 4900506.

The Electronic Medical Record – Lessons Learned

In many ways, EHRs to date have failed to deliver on their promise. There are several reasons for this. EHR acquisitions and implementations are very expensive and very time consuming. The financial costs are typically borne by physicians and hospitals, but many of the biggest benefits of an EHR flow to other constituencies, such as payors. Elimination of duplicated tests and procedures is good for patients and payors, but may adversely impact the physician's revenues. On top of that, most physicians find that productivity drops during implementation and early use of an EHR. Efficiency gains may take months or even years to realize, and even then are less impressive than the costs, as savings are never viewed as positively as increased revenue. Finally, the EHR modules that are most to physicians often must be implemented later in the process, after a core system is up and running.

Some implementations fail outright; others drag on, hindered by technical challenges or staffing obstacles such as resistance to change or the difficulty of finding computer-savvy employees. In many cases, this leads to underutilization and not reaching the system's full potential. Many people also overestimate the maturity of the technology used in EHRs. Though there are standards in place now, and more are being developed to fill gaps, extremely complicated problems are common. The efficiencies to be gained from portable, shared medical data may be impaired by the need to secure access and ensure privacy in world where patients change physicians frequently and often see many different health care providers. Insurers are eager to data-mine clinical records to better control costs, as is the government to conduct biosurveillance – but concerns about thorough de-identification remain. The potential to abuse access to EHRs also raises the specter of medical identity theft and genetic discrimination.

In spite of these challenges, EHR implementations can and do succeed. However, it is often unclear what "successful" actually means. There are currently no widely agreed upon metrics to assess the benefits of an implementation. Some benefits are simply not quantifiable; for those that are, study methodologies vary, making it hard to draw comparisons between institutions. Vendors submit projections, but these may be biased and unreliable.

This presentation and paper is intended to identify some of the lessons that have been learned in the implementation of EHRs. Much of the success of an implementation depends upon getting started properly in the early stages of evaluation and negotiation. Acquirers must understand their functional needs, the political and practical realities of their operating environment, the technical capabilities and limitations of prospective systems, and how to interpret varying pricing mechanisms. They must be well versed in the legal issues that accompany an EHR purchase, from intellectual property and warranty concerns to careful navigations through the Stark exception and Anti-Kickback safe harbors. During the implementation and after, careful thought must be given to handling potential electronic discovery requests, compliance with HIPAA and state privacy laws and data breach disclosure requirements, and addressing patient safety and fraud issues that may arise from misuse or abuse of the system.

II. Government Initiatives

A. Programs and Organizations

In his January 2004 State of the Union Address, President George W. Bush outlined a plan to ensure that most Americans have electronic health records by 2014.[2] In an effort to meet this goal, the President created a new sub-Cabinet level post within the Department of Health and Human Services (HHS). The Office of the National Coordinator for Health Information Technology (ONC) was formally established in 2005 to serve as the principal government advisor on healthcare information technology and to direct the implementation of the strategic plan to implement interoperable healthcare information technology within the nation.[3]

The Secretary of HHS also chartered the American Health Information Committee (AHIC)[4] to make recommendations on how to accelerate the development and adoption of health information technology. Currently in transition into a public-private partnership, AHIC has organized workgroups intended to spur breakthroughs in the areas of biosurveillance, consumer empowerment, chronic care, and electronic health records, as well as addressing issues of privacy and security, quality measurement, and personalized healthcare.

Interoperability has been identified as a critical element in the widespread adoption of EHRs. HHS and ONC have taken several steps to increase the level of interoperability in these systems. One such step is the creation of the Nationwide Health Information Network, which is expected to build upon regional health information exchanges (HIEs) to provide a secure, nationwide, interoperable health information infrastructure that connects patients and providers wherever they may be located. ONC awarded 9 contracts in September 2007 for a trial implementation of the NHIN.

Another step in increasing interoperability was the 2006 charter of the Health Information Technology Standards Panel (HITSP). HITSP is a public-private partnership charged with indentifying and harmonizing healthcare standards, developing implementation guidance and technical specifications for their use, and working with standards development organizations to ensure that standards are made available for use nationally.

A third step has been association with the Certification Commission for Healthcare Information Technology (CCHIT). HHS has awarded CCHIT a contract to develop and evaluate certification criteria and create an inspection process for health information technology. In conjunction with a 2006 Presidential Executive Order, interoperability has joined functionality and security as a core requirement for

[2] The President's Health Information Technology Plan can be accessed at http://www.whitehouse.gov/infocus/technology/economic_policy200404/chap3.html.
[3] More information about the ONC can be found at http://www.hhs.gov/healthit/.
[4] More information about AHIC can be found at http://www.hhs.gov/healthit/ahic/.

certification. Certification, in turn, has become a *de facto* requirement for meeting the provisions of the EHR Anti-Kickback safe harbor and Stark exception.

B. New Safe Harbors and Exceptions

It is essential to understand the impact of Federal law on the adoption of EHR technology. The Stark statute and regulations[5] prohibit physicians or their immediate family members from making referrals for designated health services to an entity, and prohibits entities from submitting claims or bills for prohibited referrals, when the physician and entity have a financial relationship. This is a strict liability law and can result in large civil monetary penalties and exclusion from Medicare and Medicaid. The Anti-Kickback statute and regulations[6] makes it a criminal violation to willfully or knowingly solicit, offer, pay, or receive remuneration in exchange for a referral for which payment can be made under a government program. Courts have interpreted the Anti-Kickback statute broadly, and in addition to civil monetary penalties and exclusion from Medicare and Medicaid, violation can result in large fines or imprisonment.

Until recently, the existence of these laws all but eliminated hospitals as avenues through which physicians could obtain EHRs. The substantial up-front cost has made physician purchases rare, and for a hospital to donate an EHR to a physician without obtaining payment for its fair market value both created a financial relationship and constituted remuneration, placing both parties at risk of violating these laws.

In October of 2006, the HHS Office of the Inspector General (OIG) and the Centers for Medicare and Medicaid Services (CMS) released final rules creating new Anti-Kickback safe harbors and Stark exceptions, respectively. These rules make it possible for a hospital[7] to provide a physician with EHR or electronic prescribing resources provided that all criteria are met. The e-prescribing exception, which was mandated by the Medicare Modernization Act, is more generous in many ways than the EHR exception although the scope of use is more narrow. Regulators have indicated that the difference is due to the statutory mandate for e-prescribing; however, the differences are intriguing given the public policy emphasis on adoption of EHRs.

1. Electronic Health Records

The EHR safe harbor / exception protects software and IT services "necessary and used predominantly to create, maintain, transmit, or receive electronic health records…" so long as 13 criteria are met. Notably, this excludes from protection any hardware, storage devices, or services used to import paper records. However, a system operating on an application service provider (ASP) model would be included, provided that the

[5] 42 U.S.C. § 1395nn and 42 C.F.R. part 411.

[6] 42 U.S.C. § 1320a-7b(b) and 42 C.F.R. part 1001.

[7] This is a generalization. Each rule has slightly different scope with regard to who may make the donation, and who may receive it. For example, the Anti-Kickback EHR safe harbor allows certain individuals or entities to both make and receive donations, whereas the Stark EHR exception applies only to donations from an entity to a physician.

other requirements are met. To fall within the safe harbor / exception, thirteen criteria must be met[8]:

- *No Hardware*.

  The EHR exception/safe harbor does not extend to hardware or storage devices. This can be a significant expense, depending on the system hardware requirements. As a practical matter, this limitation may encourage the use of Application Service Provider ("ASP") or Software as a Service (SaaS) arrangements, as the 85% subsidy is permitted for these structures.

- *Predominantly EHR*

  The software must be "predominantly" EHR software. Software with other functionality, such as scheduling and billing software, may be permitted if it is combined with, or a component of, the EHR software.

- *Provider / recipient identity*

  Under the Stark exception, the provider may be any entity that furnishes designated health services. The recipient must be a physician. Under the Anti-Kickback safe harbor, the provider may be a health plan, or any individual or entity that provides services under a government health care program. The recipient may be any individual or entity delivering health care, including a physician practice group.

- *Interoperability*

  Software must be interoperable at the time it is provided by the donor. This means able to communicate and exchange data accurately, effectively, securely and consistently with different information systems, in a manner such that the data is preserved and unaltered. Interoperability may be presumed if the software has been certified (e.g. by CCHIT) within 12 months of provision to the recipient.

- *No Restriction on Compatibility*

  The donor may not limit or restrict the ability of the system to communicate with other electronic prescribing or electronic health record systems.

[8] The Stark EHR exception can be found at 42 C.F.R. § 411.357(w). The Anti-Kickback EHR safe harbor can be found at 42 C.F.R. § 1001.952(y).

- *No recipient conditions*

  Neither the recipient nor the recipient’s practice can make the receipt of the subsidy a condition of doing business with the donor.

- *Selection of recipients by donor*

  The scheme for selecting recipients cannot directly take into account the volume or value of referrals. However, reasonable and verifiable criteria such as total hours devoted to medical practice, size of the physician practice, level of uncompensated care provided, and the physician's overall use of technology may be considered.

- *Written agreement*

  The arrangement must be set forth in a signed written agreement that specifies the items and services being provided, their cost to the donor, and the amount of the recipient's contribution.

- *Necessity requirement*

  The EHR must be necessary. This requirement is not met if donor knows, or acts in reckless disregard or deliberate ignorance of the fact that the recipient has existing, equivalent EHR software. This requirement does not preclude items or services resulting in standardization of systems among donors and recipients, provided that the standardization enhances EHR functionality.

- *No payor limitation*

  The donor cannot take any action to restrict or limit the recipient's use of the software or services for any patient or with any payor.

- *No physician's office staffing*

  The software or services may not include staffing the physician's office or assistance in converting paper medical files. Also, the system cannot be primarily used by the recipient for personal or non-medical business.

- *e-Prescribing component*

  The EHR must contain electronic prescribing capability, either as a component or as an ability to interface with another system.

- *Cost sharing*

  The donor may subsidize no more than 85% of the cost of the EHR; the recipient must pay its 15% portion before receipt of the system. The donor may not finance this cost.

- *No cheating / no cost-shifting*

  The new rules cannot be used to excuse acts otherwise prohibited by law. Costs cannot be shifted to other governmental programs.

- *Sunset*

  All subsidies must be paid prior to December 31, 2013.

2. E-Prescribing

The e-prescribing hardware, software and IT services "necessary and used solely to transmit and receive electronic prescribing information. To fall within the e-prescribing safe harbor / exception, thirteen criteria must be met[9]:

- *Donors and Recipients*.

  Under the e-prescribing exception/safe harbor, permissible donors and recipients are:
  - Hospitals may donate to physicians who are members of the Hospital's medical staff;
  - Group practices may donate to a "prescribing health care professional" who is a member of the group;
  - PDP[10] sponsors, or MA[11] organizations, may donate to pharmacists and pharmacies participating in the network, and to "prescribing health care professionals"

- *Relationship to Electronic Prescription Drug Program*
  The e-prescribing capability is provided as a part of, or is used to access, an electronic drug prescribing program that meets Medicare Part D requirements

- *No Restriction on Compatibility*

[9] The Stark EHR exception can be found at 42 C.F.R. § 411.357(w). The Anti-Kickback EHR safe harbor can be found at 42 C.F.R. § 1001.952(y).
[10] Prescription Drug Plan, as defined at 42 C.F.R. § 423.4
[11] Medicare Advantage, as defined at 42 C.F.R. § 422.2.

The donor may not limit or restrict the ability of the system to communicate with other electronic prescribing or electronic health record systems.

- *No payor limitation*

- The donor cannot take any action to restrict or limit the recipient's use of the software or services for any patient or with any payor.

- *No recipient conditions*

  Neither the recipient nor the recipient’s practice can make the receipt of the subsidy a condition of doing business with the donor.

- *Selection of recipients by donor*

  The scheme for selecting recipients cannot take into account the volume or value of referrals. Note that the e-prescribing exception does not include the surrogate measures that are permitted under the EHR exception.

- *Written agreement*

  The arrangement must be set forth in a signed written agreement that specifies the items and services being provided, their cost to the donor, and the amount of the recipient's contribution.

- *Necessity Requirement*

  The donor cannot know or act in reckless disregard or ignorance of the fact that the recipient "possesses or has obtained items or services equivalent" to the items or services the donor is providing.

3. The "CHIN" Exception

The Stark regulations contain an exception – notably, no comparable Anti-Kickback safe harbor exists – for the provision of community-wide health information systems.[12] The exception applies to items or services allowing access to, and sharing of, among other things, electronic health care records, general health information, and medical alerts for the enhancement of overall community health. Items and services may be provided by entities to physicians, without contribution, so long as they do not violate the Anti-Kickback statute or any other law or regulation governing billing or claims submission. Arrangements based on volume or value of referrals are expressly prohibited. The items and services must be available as needed to allow physicians to participate in the community-wide health information system, and must be used principally for that

[12] 42 C.F.R. § 411.357(u).

purpose, and the program must be open to all physicians, practitioners, and residents of the community who wish to participate.

4. Tax-Exempt Concerns

For tax-exempt entities, consideration must also be given to the view that the Internal Revenue Service (IRS) will take towards the provision of EHR items or services. Hospitals which are exempt from federal income taxation as an entity described in Section 501(c)(3) of the Internal Revenue Code must comply with certain requirements to avoid jeopardy to its tax-exempt status. One such requirement is that the hospital must engage only in activities that serve charitable or public purposes rather than private interests. This requirement is frequently referred to as the "private benefit test." If both public and private interests are served with respect to a certain activity, the private interest may not be served more than incidentally.

In order for the private benefit to be incidental, it must meet both a qualitative and quantitative standard. "Qualitatively incidental" means that the public benefit cannot be achieved without necessarily benefiting private individuals at the same time. "Quantitatively incidental" means that the private benefit activity is insubstantial when viewed in relation to the public benefit. In other words, the public must benefit from the activity more than the private individual does. The result is that the private benefit must be limited to the minimum level essential to achieve the community benefit. Recognizing that tax-exempt hospitals were hesitant to subsidize electronic medical records for physicians due to tax concerns, the Internal Revenue Service ("IRS") issued a memorandum dated May 11, 2007 entitled "Hospitals Providing Financial Assistance to Staff Physicians Involving Electronic Health Records"[13] (the "IRS Memorandum"). In this memorandum, the IRS noted that it would not take action against a tax-exempt hospital for subsidizing electronic health record systems if the subsidy complies with the electronic health records Stark exception and Fraud and Abuse safe harbor, so long as the following criteria are met:

- The hospital can access all information entered into the electronic health record by the physician(s) receiving subsidized items or services;
- The subsidized items and services are available to all physicians on the hospital's medical staff;
- The level of subsidy does not vary; or, the level of subsidy varies only based on criteria related to meeting the healthcare needs of the community served.

Due to questions raised in response to the IRS Memorandum, the IRS also issued a "question and answer" document, providing further guidance (the "Q&As"). In the Q&As, the IRS noted that the IRS Memorandum described a safe harbor, which was

[13] The IRS memorandum is available at http://www.irs.gov/pub/irs-tege/ehrdirective.pdf

guaranteed to protect a hospital from scrutiny so long as no private inurement existed.[14] Any arrangement that did not meet the safe harbor requirements would be reviewed under a "facts and circumstances" test. The IRS also clarified that the requirement of access by the hospital to the physician's data would be excused if providing such access would violate state or federal privacy laws or the physician's contractual obligations to patients. Further, limitations on access could be imposed. The example given by the IRS was that the hospital could be restricted in accessing patient information to those times when the patient is a patient of the hospital, and that access to billing or referral information could be completely blocked. Further, although the hospital was required to offer the subsidy to all members of the medical staff, the hospital could prioritize access to health IT and offer the subsidy in phases, so long as a formal plan for access is developed, and the sequence of access is based on community need.

The memorandum does not answer questions such as whether a hospital's subsidy will constitute taxable income for the physicians receiving the benefit, or whether private use of EHRs by physicians is an impermissible use of bond-financed facilities. Additionally, it is inapplicable to non 501(c) (3) organizations. It is also worth noting that the IRS position is more restrictive than the HHS safe harbor.

C. Other Government Assistance

A smattering of other governmental assistance, at both the federal and state levels, has arisen either to facilitate the move toward electronic records, or to directly subsidize it. Many states and localities have sponsored regional health information exchanges, also called regional health information organizations ("RHIOs") to better share clinical information among providers. As noted above, the Nationwide Health Information Network is now in trial implementation to connect such HIEs.

Other active initiatives involve the government providing direct support to physicians, rather than removing regulatory obstacles in an effort to clear the way for hospitals and other entities to do so. In 2003, the National Library of Medicine (NLM) licensed SNOMED CT, a comprehensive clinical coding dictionary, from the College of American Pathologists, and made its use freely available to technology vendors. In 2007, ownership of SNOMED CT passed to the International Health Terminology Standards Development Organisation[15] which will give even broader distribution rights in the U.S. SNOMED CT is a required standard for interoperability certification. Additionally, there are now government-sponsored free EHR software packages, such as free licenses for the use of VISTA, the Veteran's Administration EHR, and free EHRs to New York City physicians whose patient populations are at least 30% Medicaid or uninsured.

III. Acquisition

A. Structured Process

[14] The position of the IRS is that if private inurement exists, the hospital is automatically unable to take advantage of the safe harbor.

[15] See http://www.nlm.nih.gov/research/umls/Snomed/snomed_main.html.

Acquisition of an EHR system is a complex, expensive, and time consuming process. Done well, it can have tremendous benefits in efficiency, patient safety and satisfaction, and public health. Done poorly, it frequently leads to flawed or failed implementations, frustrated physicians and staff, and possibly even violations of federal or state law. It is essential to involve legal counsel in the process from the outset, and continuously throughout the process. Outside counsel may be valuable for providing subject matter expertise, with in-depth knowledge of the regulatory landscape, as well as understanding of the technology and the contractual subtleties necessary to provide adequate protection; inside counsel is essential to provide insight into the political and practical realities of a particular arrangement.

One of the first areas for a lawyer's input should be the development of a Request for Information (RFI) or Request for Proposal (RFP). As will be discussed more fully in the next subsection, the RFP should probe deeply to ensure a match between an institution's functional requirements and an EHR package's capabilities and vendor resources. But the RFP is more than a checklist or a short-answer questionnaire; the RFP and its response should ultimately be incorporated into the contract. A skilled attorney will help to frame the document to elicit the most useful information, and then to ensure that the vendor is bound to execute on its promises.

Legal counsel should also be part of the system evaluation and selection team. This can forestall long trips down dead-end pathways, such as the selection of a system that does not meet one of the EHR safe harbor / exception criteria. Even requirements that may seem obvious, such as security and access rights, have legal implications and can and should be probed in order to save weeks or months of lost effort from a nasty surprise. Lawyer's also bring important expertise in risk management issues to the table, and early involvement will help ensure that the EHR selected meets the facility's needs with respect to documentation and regulatory compliance.

Once the system has been selected, ongoing attorney involvement will facilitate and inform the negotiation process. As described below, acquisition of an EHR involves a special kind of contract that raises complex intellectual property, confidentiality, and warranty issues. Failure to involve legal counsel early in the process can sharply slow the process, particularly when IT or business staff inadvertently bargain away rights that are important for the organization to retain.

Finally, legal counsel should be involved in developing and reviewing operational policies and procedures. An EHR causes many shifts in the documentation and compliance landscape, and it is important to ensure that policies and procedures which operationalize the EHR meet compliance and risk management needs. Further, legal issues and regulatory compliance problems can arise long after the contract is negotiated; these are easiest to handle if the lawyer has maintained ongoing familiarity with the EHR.

In addition to legal counsel, the system evaluation team should include representation from key constituencies including business and administration, information technology, physicians, and end-users. A thorough understanding of the needs to be met, along with the trust of the staff, are more important attributes than technical expertise for many of these team members. Ultimately, the most successful EHR implementations have champions who can lead others through the challenges and changes that accompany a new system.

B. Functionality

At a high level, acquiring an EHR that will result in a successful implementation requires making a thorough and accurate assessment of the needs that must be met, identifying and addressing internal barriers to success, making sense of confusing pricing methods, evaluating the ability of various vendors and their systems to meet those needs and agreeing on an implementation plan, and resolving contractual, regulatory, and other legal issues. This section will address some of the important functional issues; the next will discuss legal issues.

An understanding of the key constituents' needs and goals is the first step in the acquisition process. Some needs may be described in broad terms, such as "improved reimbursement and reduced denials of claims," "reduced chart filing costs," or "elimination of predictable adverse drug interactions." Others may be described in terms of specific feature requirements, such as "archiving of clinical images," "on line retention of patient history," or particular outputs or reports to be generated. The essential thing is to identify as many of these requirements as possible, from the perspectives of not only administration and IT staff, but also the physicians, nurses, and technicians who will use the system. Requirements should be prioritized in some fashion, such as "required," "preferred," and "nice to have." Frame the requirements in functional terms, rather than specific technical terms, to better ensure a fair evaluation where each vendor can make its best showing.

A thorough workflow analysis is key to accurately assessing needs. Workflow drives healthcare, and different EHR products impact workflow differently. A clear understanding of workflow permits better selection and easier implementation of an EHR. Often a formal evaluation of workflow reveals variations from policy in actual performance of tasks. Identifying who does what, when, where and how permits the EHR implementation to leverage current practices while identifying new efficiencies.

Next, the current electronic environment should be assessed. Existing systems may require interfacing, upgrading, or replacement and data may need to be migrated/converted to the new system. New input devices may be desired, such as PDAs, tablet PCs, or voice recognition.

Once the institutional needs and challenges have been identified, a request for proposals will generally be sent to several vendors whose EHRs appear through advance research to meet the requirements. However, one of the most fundamental response elements – pricing – is typically very difficult to compare between vendors. There are several causes for this. EHR licenses come in many different flavors, such as:

- Concurrent user (pay for the peak number of staff that could be active)
- Named user (pay for every computer upon which the software is installed. or every authorized user)
- Enterprise (pay one fee for unlimited use)

To add confusion, systems may be delivered in a variety of fashions that can impact the price. They may be installed on local machines connected to a central repository (client-server), installed virtually via a technology such as Citrix, or accessed over the Internet via an Application Service Provider (ASP) / Software as a Service (SaaS) model. Each of these methodologies involves different degrees of end-user training, technical support resources, hardware requirements, and flexibility. For example, a virtual implementation over Citrix may eliminate the need to replace aging desktop computers, dramatically reduce application upgrade costs, and provide physicians with the ability to work from home; but server requirements are substantially greater, and the need for sophisticated and specialized IT support staff may be prohibitive.

Another way quotes may vary substantially is in their inclusion or exclusion of hardware. Hardware can often be 20 to 30 percent of the first-year cost of an EHR, and vendors typically follow one of three approaches to it: resell it directly (or through a third-party) and include in the pricing; provide a budget estimate and specifications, allowing the acquirer to use its own preferred hardware vendor; or omit a hardware budget entirely. Even when comparing quotes that include hardware, major variances can arise due to system requirements, proposed architecture (compare ASP to virtual implementation via Citrix), built-in redundancy and "hot swappable" backup capability, inclusion of upgrades to or replacement of workstation computers, and ancillary devices such as bar code printers and readers, cameras and scanners, mobile input devices and the like.

Pricing will also be impacted by the number and complexity of interfaces to other systems, the budget allowed for customization of screens, templates, and specialized functionality, and the inclusion or exclusion of optional modules or data conversion services. As with any transaction, a healthy dose of skepticism goes a long way with EHR purchases. Although buying unnecessary components at high cost is clearly to be avoided, a low priced system that fails because critical items or services were omitted benefits no one.

Finally, initial training and ongoing technical support and software upgrade costs must be considered. Vendors differ in the location (onsite vs. offsite) and scope of training services offered, and the complexity of the EHR and its ease of use will likely affect this cost as well. Similarly, the level of support services and the frequency of scheduled upgrades will affect the price significantly. Ongoing costs can range from 10 to 40 percent of the one-time implementation costs, depending on the level of service required. Specific recommendations on contracting for services are included in the next section.

Typically, after the evaluating RFP responses, those systems with the most promise will be selected for further review. This usually involves one or more technical demonstrations at the acquirer's location, site visits to locations where the vendor has a currently active system, and numerous business, operational, and technical conferences to exchange information and ensure a good fit. During this process, the system evaluation team should be asking detailed questions about not only features, but also ongoing operational issues. Examples include:

- *Is the version being demonstrated the same one that will be purchased?*

  Occasionally vendors will show new versions that have not been completed or released – and in actuality may never be. Such systems are derisively referred to as "vaporware."

- *How much scheduled and unscheduled downtime will occur, and how do users operate when the system is off-line?*

  All software requires periodic maintenance, and computers unfortunately do go down on occasion. Redundancy and disaster recovery can and should be built in to the system, especially for mission-critical applications; but this rapidly increases costs. The evaluation team should ensure that the intervals, start time, and duration of scheduled maintenance is acceptable, and assess the viability of offline (electronic or paper) operations should they be necessary.

- *How will the EHR accommodate growth and changes in functional or regulatory requirements?*

  EHR implementations are costly and time consuming. Selecting a system that meets not only current, but also future needs, is essential. Growth should be assessed not only in terms of number of licensed users, but also strategic change. Even if the institution has no active plans for mergers or acquisitions, consideration should be given to the ability to expand to serve a new hospital site or joint venture, whether in the same region or outside it, or to integrate with other systems should the institution itself be acquired. The ability of the system to handle changing functional requirements, whether they are evolving areas of medicine such as genetics, or new ways of communicating with patients such as secure messaging, should be evaluated. The system must be capable of remaining compliant, through upgrades, with all laws and regulations.

Vendor responses to such questions should be carefully recorded and compiled for later incorporation in the contract, as discussed below.

Finally, the implementation plan should be outlined prior to final selection of a system. Although specific details can be filled in at a later point, the system evaluation team must have a solid understanding of when an implementation project could be started and a projected duration, including major milestones such as completion of interfaces, data conversion, delivery of required customizations, and sequence of module activation. The preliminary project plan should identify vendor responsibilities, and often overlooked, institutional responsibilities such as provisioning hardware, installing required infrastructure like increased network capacity, and selecting an implementation team and project manager. As with the RFP and its response, the implementation plan should be incorporated into the contract.

C. Legal Issues

As noted above, legal counsel plays important roles in evaluating and selecting an EHR, negotiating the contract, and planning for legal issues that may arise during the ongoing use of the system, as well as investigating and responding to violations if and when they occur in the use of the EHR.

One of the most critical responsibilities of an attorney during the selection process is to evaluate the regulatory compliance of EHR systems under consideration and of proposed entity-physician access arrangements. Careful attention must be given to whether the system itself meets the EHR safe harbor / exception. Does it include an e-prescribing component? Has it been certified by CCHIT, which establishes that the interoperability requirement has been met – and if not, are common interoperability standards used, such as HL7, SNOMED, and DICOM? Does the system meet requirements for data integrity and exchange? Is the EHR functionality primary, or are other components of greater significance? In some ways, the attorney must function as a guardian and eliminate systems that may have great allure to the physicians and staff, but would risk the institution's inclusion in federal programs such as Medicare.

Similarly, legal counsel should carefully scrutinize the arrangement under which the system will be made available, if it is being subsidized or donated, and draft a written agreement between the parties. For EHRs, the 15% physician contribution is a minimum requirement, and must be paid in advance – without financing from the hospital – prior to receipt of the system. Calculation of the donor's cost and documentation of receipt of payment is critical. The system must be offered without donor conditions or payor limitations, and the arrangement may not be based directly on value or volume of referrals nor offered in response to a recipient's condition of doing business. The system must be necessary and non-duplicative.

In addition to the Stark and Anti-Kickback issues, legal counsel must evaluate both the system and the donation arrangement for compliance with other relevant regulation, such as IRS 501(c)(3) guidance on private inurement. Of particular concern are compliance with HIPAA and with state confidentiality laws, as well as with any institutional policies such as minimum password strength and frequency of changes. The system must incorporate adequate security mechanisms to prevent unauthorized access and detailed auditing of user activity that facilitates detection and investigation of breaches.

It may go without saying that legal counsel should play a primary role in negotiation of the EHR licensing contract; what bears repeating, however, is that these are specialized contracts and require particular expertise in order to adequately protect the acquiring entity. If the recommendations in the previous section have been followed, by the time negotiations begin, the attorney will already have an RFP and the vendor response to it, an implementation plan, and a list of vendor responses to the evaluation team's questions.

The vendor will typically supply a standard contract as well, but such contracts are vendor-friendly, often omit key terms and invariably need to be modified to protect the acquirer. As noted, the RFP, response, and implementation schedule should be incorporated by reference into the contract. So too should be any marketing materials supplied by the vendor. Standard contract terms that conflict with vendor responses to questions should be modified. Careful attention should be paid to the definition – or lack thereof – of key terms such as "user," "activation date," and "equipment"; some poorly drafted contracts will include conflicting definitions, particularly when the "contract" is actually a set of separate documents such as a software licensing agreement, a hardware purchase agreement, a implementation and training services agreement, a network access agreement, and so on.

Beyond the basics, several issues deserve particular attention. Intellectual property rights are critical for the customer. Scrutinize the scope of license granted – can the customer make a copy for archival and back-up purposes? Can it retain a copy after termination of the license, to allow the customer to access information in the system? If the customer is to have the ability to develop customer-specific templates, modify screens, create reports, or modify source code, ownership of the changes must be addressed; so too should the ownership of any software customizations purchased with the system. Another important consideration is infringement of third party rights. The vendor must include a warranty of non-infringement of others' intellectual property, and should provide that the vendor will indemnify the customer against claims of infringement arising from the possession or use of the EHR.

The customer must also protect its own intellectual property that will be stored within the EHR, particularly if it is an ASP or Software as a Service system in which the customer does not own the hardware upon which its data is stored. In such a configuration, the contract should specify the vendor's backup and archival responsibilities, including rotation of backup media and testing to verify reliability. In the event that the contract is terminated, surviving provisions must be incorporated for the return of customer-owned data. Similarly, the contract will typically include confidentiality provisions, but these often need to be strengthened (with regard to the customer's data) and weakened (with regard to remedies arising from the customer's disclosure of confidential vendor data). Consider carefully any provision that permits vendor to use customer's data for vendor's own purposes. Finally, terms requiring the vendor to comply with HHS requests for access to books and records, or with state data breach disclosure laws will likely need to be added.

Typically, the vendor will combine a front-loaded payment schedule ("100% of the purchase price is due upon execution…") with extremely limited remedies in the event of termination or breach. Such terms should be negotiated. Payments should be linked to verifiable milestones, subject to customer acceptance of a given deliverable. The acceptance procedure should be defined, and acceptance in stages should not preclude the customer from rejecting the EHR if, when fully implemented, it fails to comply with specifications or performance warranties. Remedies should adequately address outright failure or partial failure of the system and not be limited merely to refund of the license fees paid.

Vendor-supplied contracts will usually aggressively disclaim most warranties related to performance. This is a critical area for the customer, since it can leave an institution without recourse if the software never works, or works for a while and then stops working. The vendor should warrant that the system configuration and capacity, as recommended to the customer, are complete and conform to the requirements set forth in the RFP. It should warrant compatibility with necessary hardware and software, including operating system, database, and third-party applications. Uptime and response time claims made during the evaluation process should be warranted.

The contract should include or reference a defined procedure for obtaining technical support, including response time and escalation procedures for problems of various severity levels. A support clause should provide for automatic escalation of problems that remain unresolved after a specified interval, and should require the vendor to continue to work toward a long-term solution even after a workaround has been implemented.

Other terms that frequently require addition or modification include:

- Warranties that the software actually exists in usable form and will remain current for a specified time or be upgraded at no charge

- Warranties that the EHR does not contain surreptitious code (backdoors) or viruses

- Warranties of competence in the provision of services, and that appropriate liability and worker's compensation insurance policies are and will remain in effect

- Warranties of compliance with federal and state law, including a provision that neither the vendor nor any of its agents or officers have been debarred from participation in any government healthcare program

- Warranties of adequate capitalization and solvency, and that financial statements comply with Generally Accepted Accounting Principles (GAAP) and are true and complete.

- Provision for escrow of source code and conditions under which it may be accessed

- Disclaimers, e.g. of UCITA, and favorable choice of law. Consider arbitration provisions

In addition to contracting issues, legal counsel should consider how the system should be structured in order meet the regulatory and standards-setting body requirements for a legal electronic medical record.[16] The legal EHR is a subset of the entire patient database that serves as the legal record or care for the organization. It must be producible upon request, in a method that minimizes the risk of security breach and ensures patient privacy. Many EHRs have capabilities which are helpful to clinicians, but are not part of the traditional legal medical record. These capabilities should be identified and technologically segregated.

Since the revision of the Federal Rules of Civil Procedure in 2006 to include extensive electronic discovery provisions,[17] new complications have arisen in the use of EHRs. In the event of litigation, attorneys must decide how to comply with a discovery request for electronic records. Not only current patient data, but also original and corrected versions of records, deleted records, emails, and EHR alerts and prompts are all potentially discoverable. Depositions can be expected to take longer, and responses will require a thorough understanding of the processes and functionality of the EHR. The institutions record-retention policy must be updated to address electronically stored data, and the system must be capable of being frozen in an unaltered state to prevent the spoliation of evidence in the event of a discovery request.

IV. Implementation and Operation

A. Personnel Issues

People are among the greatest obstacles to the successful implementation of an EHR. Frequently, fear of change alone is a tremendous challenge. Some users would simply prefer to do things "the way they have always been done"; others may lack basic computer skills entirely and not feel that they can understand how to use an electronic system. After hearing about the expected efficiency gains from the use of EHRs, some staff may be genuinely afraid of being replaced by computers. Doctors, in particular, may resent the feeling that a computer is telling them how to practice.

[16] For more information, see http://www.himss.org/content/files/LegalEHR_Flyer3.pdf.

[17] The revisions were submitted to Congress on April 12, 2006, and took effect on December 1, 2006. See http://www.uscourts.gov/rules/Letters_Orders.pdf. For an annotated summary of the changes, see http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

Especially among physicians and staff whose compensation is tied to output, such as numbers of lines transcribed, loss of productivity is a very real concern. Already overworked doctors may rightfully question who will see patients while they are being trained, and how they will find the extra time to prescribe medications electronically instead of jotting a quick note on a pad of paper. Indeed, concerns of lost productivity are well-founded, at least in the short term. Reports of decreases in productivity ranging from 20 to 50% in the first few months of a system's implementation are not uncommon. Of course, as comfort level and experience increase, a well implemented EHR should actually *increase* productivity, but this can be hard for physicians and staff to believe at the beginning of a project.

Other concerns can raise physician and staff resistance as well. Physicians may fear that the use of portable or online medical records will make it easier for patients to doctor-shop, or for other physicians to steal patients. And there are often substantial communication barriers between information technology staff who do not understand clinical requirements, and clinical staff who do not understand computers. Indeed, technically savvy clinical personal such as nurses and medical technicians are highly sought after as employment candidates by EHR vendors, as well as by providers.[18] To address this challenge, many colleges are now offering degree programs in fields such as Health Information Technology.[19]

In order to succeed, an implementation must plan for these obstacles and ensure that sufficient clinical and technical resources are available and allocated both during the transition and to assist with lost productivity after cutover. Physicians and staff need to feel that they have a voice in the project so that they develop a personal investment in its success, and ideally there should be a respected champion among them to help push through the challenging times.

B. Technical Issues

As noted above, a host of technical issues arise in the selection and implementation of an EHR. Decisions must be made including whether to use a local or ASP model, what input devices (such as PDAs) will be used, etc. Settling upon a system architecture is in many ways just the beginning. Large-scale implementations, particularly across multi-site operations, will often require upgrades to network infrastructure. Bandwidth may need to be increased, particularly if document imaging, clinical imaging, or audio data are to be transmitted. Such changes must be identified early on, since slow-moving telecommunications providers may need to be engaged, or specialized equipment may be required.

Among the most complex and time consuming technical challenges are the development of interfaces between existing systems and the new EHR. Although most vendors have standard interfaces, in reality even "standard" interfaces require substantial

[18] Christopher Rowland, *Hospitals' Move to E-files Spurs a Labor Shortage*, BOSTON GLOBE, May 14, 2007, *available at* 2007 WLNR 9246269.
[19] E.g., http://www.devry.edu/programs/health_information_technology/about.jsp.

configuration and customization; true "custom" interfaces may take months of programming and testing. To be sure, one of the advantages of a comprehensive, modular EHR system is that the number of interfaces may be reduced by using a single-vendor solution. But it is a rare implementation that can avoid them entirely, and although standards for data exchange, such as HL7 and XML, exist and are widely used, vendor implementation of the standards varies. Because interoperability is a primary objective of the NHIN, there is a substantial push toward more uniformity and greater use of standards.

Handling legacy data is also a challenging task. Institutions may be changing over from one EHR to another, resulting in the need to convert electronic data into the new system. Though this is a complex and often imperfect task, EHR vendors and specialty consultants are capable of performing it. However, paper chart data poses an entirely different problem. Decisions must be made as to how to handle this legacy data. In some implementations, the data (or a subset of only certain data elements or temporal divisions) is manually entered into the new system. In others, the EHR may only contain a flag indicating that there is prior paper history, or have no indication at all. Other systems choose to scan paper records into the new EHR. Whatever solution is selected, it will be imperfect and challenges are sure to arise along the way.

C. Security and Privacy

Security breaches can result in extremely sensitive data being compromised. Even without the use of EHRs, many patients do not seek reimbursement of certain types of care, such as mental health treatment or treatment for sexually transmitted diseases, out of fear of adverse employment consequences or public disclosure.[20] Medical identity theft is a rapidly growing criminal problem with the potential to affect millions of Americans as EHRs become more ubiquitous.[21] Cross-cutting identity theft is the problem of unique identification of patients: mixing patient medical data could have disastrous results, but no secure, unique medical identifier as yet exists. Privacy is a topic of primary importance to the government as it moves forward with the Presidential goal of widespread EHR adoption, and AHIC has established a cross-cutting workgroup to address the topic.[22] In the meantime, insurers are eager to data-mine (hopefully) sufficiently de-identified patient data to better control costs.[23]

Thus ensuring the security of sensitive information is among the paramount concerns of EHR implementers. Compliance with HIPAA is obviously a requirement. Equally important, but less obvious, are regulations setting authenticity and integrity requirements for electronic signatures and records,[24] diagnosis or disease specific

[20] See Jim Landers, *Medical Privacy in a Digital Era*, DALL. MORN. NEWS, Nov. 21, 2006, *available at* 2006 WLNR 20205146.

[21] See J. Scott Orr, *Critics Say Medical Database Poses a Risk*, OLYMPIAN, July 10, 2007, *available at* 2007 WLNR 13026898.

[22] See http://www.hhs.gov/healthit/ahic/confidentiality/.

[23] *Medical Privacy in a Digital Era*.

[24] 21 C.F.R. part 11.

confidentiality regulations such as for drug or alcohol treatment,[25] and state laws imposing specific disclosure limitations under certain circumstances such as where minors are involved, for mental health treatment, or testing or treatment for HIV/AIDS.[26]

Some security challenges are particularly complex. For example, managing permissions to access data where patients are shared across provider networks, or between a hospital and a physician joint venture, is a daunting task. Since confidentiality is an ongoing commitment, the problem does not end when the patient relationship ends; in fact managing access to former patients may be even more complicated. Furthermore, relationships are dynamic and therefore access to new providers must be granted on an ongoing, sporadic basis. Unfortunately, technology controlling access is less mature than one might wish; truly effective context-based and role-based access is very hard to achieve.

Adding to the challenge, not only providers, but patients themselves want access to their medical records. It can be difficult to convince healthcare providers of the need for encryption, strong passwords, and other security precautions; helping consumers understand and implement these precautions can be even more challenging. Consumers are also harder to train, and more susceptible to human engineering and phishing attacks; without IT personnel to assist, many consumers do not update virus definitions and become infected even when they have anti-virus software available.

Even where the challenges of *permission* have been met, providers must be able to *access* the electronic data. No standard has yet emerged for doing so, though proposals range from centralized on-line databases such as HIEs to patient-carried smart cards with varying amounts of data storage.

Fortunately, some security challenges are not so complicated. Although easily overlooked, physical security remains a critical front-line defense. Server rooms should be locked and access to them limited; portable devices such as PDAs and laptops should be encrypted and accounted for. The widespread prevalence of portable storage such as flash drives poses a special risk, and it is likely that new methods of encrypting data and locking out peripherals will be developed.

In recognition of the increasing mobile use of computing assets, DHHS has issued Security Guidance for Remote Use.[27] Centers for Medicare and Medicaid Services is very concerned about the security risks posed by remote access to PHI, and in fact notes that " covered entities should be extremely cautious about allowing the offsite use of, or access to, EPHI…"[28] Risks associated with accessing, storing and transmitting ePHI are considered, and risk management strategies addressed. One lesson is clear – covered

[25] 42 C.F.R. part 2.

[26] See, for example, Mich. Comp. Laws § 333.5131 (imposing strict limitations on disclosure of records relating to HIV/AIDS infection, and providing criminal sanctions for their breach).

[27] Available at http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf

[28] *Id.*

entities need to carefully consider the risks, and take steps to protect ePHI that is accessed remotely.

D. Risk Management Considerations

In many EHRs, substantial customization is possible. However, this poses the challenge of deciding how information is to be entered into the system, and how much automation is appropriate. Data entry templates can cut down errors and reduce costs by making many tasks faster; however, they may not allow for capturing the nuance of particular patient concerns. Similarly, macros or exploding text can greatly accelerate transcription but may leave doctors with little room to choose precise wording. This can lead to increased risks of malpractice or claim denial. Cloned and replicated content can save a great deal of time but raise similar problems. If too much information is replicated from one visit to another, there can be little to distinguish patient visits. And certain information, such as patient demographics or insurance, may be appropriate candidates for cloning from records of prior encounters, but cloning clinical data may raise reimbursement or fraud concerns.

Involvement of risk management and legal counsel early in the process of selecting an EHR can save a great deal of grief in the long run. Changes in workflow, presentation of information on multiple screens, and complicated mechanisms to correct errors in entry can lead to mistakes that threaten patient safety. Lack of flexibility in clinical description, by eliminating free text, can limit the ability of a clinician to convey a clear picture of the patient's status. On the other hand, excessive reliance on free text entry can lose hoped-for efficiencies, and complicate care by use of non-standard terms. Alerts of contraindications and interactions are important, but if alerts are too sensitive and include innocuous interactions, they can also lead to "alert fatigue," where the provider simply clicks "OK" without focusing on the content of the alert. Finally, decision support systems can assist providers with complex diagnoses, but also need to be flexible enough to recognize that the human condition is complex, and patients may not present with textbook symptoms.

Conclusion

In the end, the EHR needs to support providers in the complex process of providing high-quality, efficient healthcare. Through careful planning and implementation, EHR's can contribute to patient safety. Involving legal counsel, both in-house and outside, early in the process can contribute to a successful, positive contracting and implementation experience.