Annals of Health Law

Volume 19
Issue 1 *Special Edition 2010*

Article 37

2010

The Challenge of Implementing Interoperable Electronic Medical Records

James C. Dechene

The Challenge of Implementing Interoperable Electronic Medical Records

*James C. Dechene**

Encouraging health care institutions to implement a system of Electronic Medical Records (EMR) has been a prominent public policy objective for several years. The federal government has provided financial incentives as well as exemptions and safe harbors from Anti-Kickback and Stark Law provisions to encourage the widespread adoption of EMR by health care providers. A key feature viewed as essential to EMR is interoperability, generally viewed as the ability of an EMR generated by one provider to be seamlessly accessed and integrated into the EMR of a different provider. Indeed, patients may one day have their complete EMR on a flash drive that they may take to any provider so that the patient's current provider has full access to the patient's complete medical history.

The promise of having an integrated medical record for each patient is substantial. Each treating physician would have access to all of the prior test results and medical history of the patient. Costs associated with duplicative and unnecessary testing potentially can be eliminated. The risk of providing treatments that are not necessarily in the best interest of a patient with a medical condition that was diagnosed by another provider earlier but is unknown to the current provider can be reduced. Each treating physician can have access to the overall care plan and treatment strategy pursued by prior physicians. Consequently, the implementation of interoperable EMR systems often is viewed as a primary driver for expected reduced national health care costs and improved quality of care.

Unfortunately, there appears to be a significant gap between the promise

---

* James C. Dechene has over 25 years experience in representing health care providers on a wide variety of health law matters, both in a large international law firm and as General Counsel for an Academic Medical Center. He has taught and written widely on a variety of topics, including Fraud and Abuse and Stark, Medicare, Medicaid and other healthcare reimbursement systems and other healthcare regulatory matters. The views expressed herein are his own and should not be attributed to any other organization or entity to which Mr. Dechene has been affiliated.

of EMR as envisioned by policy makers and the reality of EMR as currently offered by vendors. Attorneys and policy makers working with providers seeking to implement EMR need to understand the gaps and challenges of implementing a truly interoperable EMR system. This article identifies some of the issues that providers are facing in implementing EMR systems. One thing that should be clear at this point in the development of EMR is that the goal of a seamless, interoperable EMR system is still a distant dream. Policy makers should consider resolving some of the issues identified in this article through a process of standardization that helps facilitate the goal of seamless, interoperable EMR.

I. TECHNOLOGICAL CHALLENGES

Perhaps a starting point for understanding the challenges of EMR is to understand on a non-technical level how current EMR systems are developed. Since most lawyers do not have substantial expertise in the technology of EMR, they may not appreciate some of the difficulties posed in developing a seamless, interoperative EMR system. This section describes, on a high level, some of the challenges of connecting one EMR system to another system.

To the uninitiated, an EMR may seem a relatively straight-forward electronic database that can be easily integrated. In concept, an EMR is essentially an electronic database that includes an organized version of what historically has been part of the written medical record: a medical history, physician orders, physician notes, nursing notes, laboratory test results, radiological images, specialist physician notes, etc. An EMR would exist if all of the documentation were entered electronically into a database that organized medical history, physician orders, physician notes, nursing notes, and laboratory and other test results.. If all EMR systems had a common structure for gathering such information, it would be rather straight-forward to take information from one EMR and merge it in a consistent way with comparable information from another EMR.

In practice, however, EMR systems are much more complex. As presently designed, EMR systems attempt to merge together several different information technology (IT) systems in use by health care providers. The EMR system includes systems for patient registration (capturing patient demographics and third party payor information, pre-authorization where required, etc.), systems for physician ordering of all ancillary services (pharmacy, laboratory, radiology, etc.), systems for transmitting the orders for ancillary services and the results of the ancillary services, systems for billing all services electronically to third party payors and patients, and other IT components used by providers. An EMR architecture that includes all of the IT functions needed by the provider is a

good deal more complicated than an electronic database limited to the medical record.

A logical place to begin this discussion is with the ordering piece of the process. Each provider will have a unique selection of options for ordering. If a physician is ordering pharmaceuticals for a patient, the options incorporated in the EMR system will likely be limited to the formulary adopted by the provider. As each provider is likely to have a somewhat unique formulary, use of a common EMR system for multiple providers is problematic. No provider will want to include drugs that are not on that provider's formulary in its order sets.

Taking the matter further, the EMR system will essentially reflect the means by which a particular provider or medical facility cares for patients with specific medical conditions. Treatment algorithms for each medical condition are essentially coded into the EMR system. Some of those treatment algorithms may be viewed as proprietary. The treatment algorithms, and options available to physicians for treatment under the EMR system, may differ substantially among providers. The types of treatment options available at a sophisticated academic medical center are likely to be much broader than the options at a community hospital. Some of the differences reflect the technology available at a tertiary or quaternary facility versus the technology available at a community hospital. Other differences may reflect the specialists available at a particular facility. Contrary to what would normally be expected, these differences do not necessarily mean a difference in the quality of services provided. Rather, for the most part, the differences simply reflect somewhat different services.

The key point is that the optimal integrated IT system for each facility is likely to be unique. The more treatment options available at a particular facility, the more unique the optimal system will be. Forcing a system optimized for one facility onto any other facility is problematic. While systems can theoretically be tweaked to accommodate multiple facilities with unique needs, this adds complexity to the programming required and multiplies the odds for systemic problems.

For example, if the same integrated EMR system is used for three separate facilities, each of which has its own unique formulary, there will need to be a master file that includes all of the drugs on any of the formularies. Than, the system needs to be programmed to recognize that if a physician is ordering a pharmaceutical at one facility, the physician will only have access to the portion of the master file that is limited to the formulary for that facility. If a physician practices at multiple facilities and logs onto the system from a different facility, the physician will pull up an order set for the wrong facility, and may order drugs (or other treatments) that are not available at that facility.

An EMR system that imbeds all of these unique components and requires

all other systems that connect to use the same components has the potential of hindering the principle of interoperability rather than facilitating the type of interoperability that policy makers no doubt envision. If the only way to adopt an interoperable EMR system is to pick a particular IT architecture, the EMR will only be interoperable with systems that utilize the same IT architecture. Within that IT architecture, all providers will be forced into the order sets, practice structure, charge master design, etc., of the sponsoring system. Most important, locking providers into a particular IT architecture means that each of the providers choosing that architecture will in effect be locked into connections with just one hospital system.

While there may be competitive advantages associated with a healthcare delivery system built around a limited number of mutually exclusive competing integrated healthcare systems, it is not at all clear that such a model is the most competitive and cost-effective. In any event, the decision as to whether or not our delivery system should be structured around a limited number of mutually exclusive competing integrated delivery systems should be made on the basis of something other than the IT architecture for EMR, which health care IT vendors are developing. Yet, a number of the EMR systems in development today are pushing us in the direction of a limited number of mutually exclusive integrated delivery systems.

Nor is this a case where technology is forcing healthcare into a box. The issues identified above relating to integrating EMR systems would not be a problem if either (1) the EMR system were not embedded into all of the other IT systems used in healthcare facilities; or (2) interoperability were determined at a level other than at the entire system level. However, the architecture of many EMR systems currently has both features. An architecture which does not facilitate easy interoperability with completely separate systems poses a challenge to the goal of universal adoption of EMR in a manner in which EMR from any facility is readily made available in a seamless way to every other provider in the country.

There is a potential solution to this dilemma. Given the substantial amounts of subsidies that the federal government is prepared to dispense to encourage the adoption of EMR, it would behoove policy makers to consider imposing conditions on these subsidies, and limits on safe harbors and exceptions to EMR systems designed with a truly open architecture.

The solution entails viewing the EMR system as two separate components. The first component is the IT architecture around the customized health information systems utilized by any individual provider. That IT architecture is the aspect of the system that will, and should, continue to be tailored to each facility. The order sets, charge master codes, security settings for ordering and entry of orders for each unique health system will be embedded within the IT architecture. Each health system

should incur the costs of its own architecture, without a subsidy from potential partners.

The second component in the EMR system is the individual medical record itself. The record should be viewed as separate and distinct from the manner in which the record was created. Any EMR from any system should be readily readable and integrated into any other EMR system in use by any other provider. To achieve that result would entail imposing substantial standards and requirements on the individual record component of EMR. Those standards should identify key universal components for all EMR: medical history, physician notes, physician orders, nursing notes, diagnostic test results (including standards for clinical laboratory test reports, radiological imaging test results, storage of underlying images, ultrasounds, EKGs, etc.). Then, for each component, there should be either a common format for saving the information or a common data protocol in which all of the information is saved.

Requiring adherence to standards for all of the components of the EMR record itself (as opposed to the overall IT system which is used to build the individual EMR record) should facilitate development of systems that can pull up and integrate the EMR entries created by any other EMR system into the EMR system utilized by a particular provider. The test should be whether (1) any EMR system can pull up and seamlessly incorporate into the EMR record of the provider using the system all of the components, in the right format and (2) whether the EMR saved by any EMR system is in the standard format so that all of the components are recognized and saved by any other EMR system that utilizes the EMR standards. The system should save all diagnostic test results in the same place, all physician notes in the same place, all nursing notes in the same place so that any physician has ready access to the complete medical record. It should not be viewed as sufficient if all of the records are available, if all of the other components, such as diagnostic test results, are not also saved and incorporated in the place designated for each component.

If each EMR system utilized the same national standard then patients could readily move from one provider to another without being disadvantaged if the new provider does not have full and seamless access to the patient's complete medical history. The promise of EMR likely will not be satisfied unless there are clear standards on the format and location of each component of each EMR record entry.

II. LEGAL IMPEDIMENTS

The second impediment to the promise of EMR is a conflict between federal and individual state limitations and restrictions on medical records. States frequently impose strict limitations on the release of certain

information, such as information relating to mental health diagnoses and care, HIV status and treatment, and information regarding minors. Similarly, there are federal laws that limit the disclosure of certain health information. As the EMR technology moves in the direction of open access to the entire medical record by any treating health care provider, there are substantial concerns as to whether the open access will put a provider in violation of some of these requirements.

If, for example, a state law strictly limits the disclosure of any information related to a mental health diagnosis or treatment, providers may need to block or pull out EMR data that relates to such matters. Of course, there are troubling policy and quality concerns associated with blocking another treating physician's access to such information. One would think that knowledge of a mental health diagnosis or a prescription to certain behavioral health pharmaceuticals is as important to a subsequent treating physician as any other patient information. However, some state laws limit and protect certain types of medical information. Any provider in a state that prohibits or restricts disclosure of some EMR information faces challenges in constructing a truly seamless EMR system.

In some cases, providers have addressed the situation by "locking down" some protected portions of the EMR. While such a solution may be necessary to keep the provider in compliance with applicable law, it limits the utility of EMR. There also are challenges associated with a lock down of only a portion of the record. For example, pulling chart entries for physician notes relating to behavioral health treatment would not solve the problem of blocking access to orders for behavioral health pharmaceuticals. Blocking a portion of pharmaceutical orders would not protect against the release of information in some diagnostic tests that might disclose that a patient either had a particular diagnosis, or that the patient was on certain medications.

It is quite challenging for a provider seeking to have interoperable EMR to comply with some of the restrictions on the disclosure of certain information. It is even more challenging when providers may be given access to information from providers in another state, as states may impose different restrictions and limitations on the use or further disclosure of such information. Clearly, if the promise of EMR is to be realized, there should be some legislative and regulatory attention given to these issues.

In view of the variety of differing laws of multiple jurisdictions, it would seem that the most appropriate solution would be a federal law that clearly preempts conflicting state laws. To the extent that federal policy intends to encourage the deployment of EMR on a basis that permits patients to have the complete medical record available to any provider that they see, Congress should expeditiously enact a statute that sets forth reasonable requirements for maintaining the confidentiality of records, while

permitting any health care provider with appropriate access (and in the case of treating physicians, most likely full access) to the complete EMR record of the patient.

Absent a federal law protecting the release of the full EMR to another treating provider, providers will need to "protect" substantial portions of the EMR from disclosure to other treating professionals. In an effort to avoid violations of various restrictions, providers can be expected to protect portions of the medical record over-inclusively. The only practical solution to this barrier is a broad federal law that explicitly preempts any conflicting state, local, or other federal laws that might preclude release of certain portions of the EMR.

III. PRIVACY CHALLENGES

The third barrier to achieving the promise of seamlessly integrated EMR is protection of privacy. Once again, the solution to this challenge will require a federal legislative fix. The challenge of privacy stems from EMR vendors adopting their own views on protecting the privacy of the EMR. Additionally, since the EMR vendor is generally not the party that would be accountable for a violation of privacy requirements, the legislative solution may require creativity to encourage EMR system vendors to offer security features that match federal requirements.

In the absence of legislation in this area, EMR vendors are developing their own systems to permit access to EMR by any healthcare provider who is treating a patient. These EMR everywhere products generally establish a protocol designed by the EMR vendor. Healthcare providers often view the security/privacy protocols established by EMR vendors as inadequate. In the absence of legislation that both gives providers a privacy "safe harbor" and encourages EMR vendors to meet the federal requirements for any safe harbor, health care providers will be caught between privacy concerns and the pressure to participate in EMR products that reflect the promise of seamless EMR systems.

Of course, EMR vendors can be expected to both pressure their clients to utilize their EMR everywhere products and to implement commercial security systems that may not meet the enhanced privacy security systems for medical records. Indeed, some EMR products permit access to medical records if the requestor has access to name, address, birth date and one or two other pieces of information to which a any "snooper" may have access. Because the security system for EMR everywhere access generally must be standard for all users of the system, purchasers of EMR systems generally lack the commercial leverage to dictate the security system. Federal standards are the only potentially effective leverage against vendors. Perhaps, then, access to federal funds to support the development of EMR

can be conditioned on EMR everywhere products meeting defined federal standards for security.

Even with federal security standards, there still will be instances of "snooping" in patient records. Federal law should determine who bears the responsibility for such violations. If the promise of EMR is to be fulfilled, legal responsibility for unauthorized disclosure or access should be limited to the person who obtained unauthorized access, and perhaps the employer of any person obtaining access if traceable to procedural deficiencies of the employer. A provider who participates in an EMR everywhere system that satisfies potential federal standards for security should not be held accountable for unauthorized access by someone not under the control of the provider. If the initial provider faced legal responsibility for access to the provider's records by persons working for another entity, who are in no sense under the control and direction of the initial provider, the risk of security breaches would be too great to facilitate EMR access. If public policy intends to facilitate ready access to EMR records, providers who participate in EMR everywhere services that meet federal security requirements should be immunized from claims for breaches by others not associated with the provider.

IV. CONCLUSION

EMR systems hold much promise for increasing the quality and the cost-effectiveness of care. IT support behind EMR systems can assist in improving care by creating consistent plans of care and medical practices. However, if the promise of EMR is to be fulfilled, policy makers should consider and appropriately address the issues identified in this article.

Perhaps the best way for policy makers to craft approaches to these issues would be to interact with healthcare IT professionals in order to understand how prominent EMR systems are constructed. The goal of any policy solution should be to encourage and support the adoption and use of EMR systems. At the same time, policy should seek to be as neutral as possible with respect to the impact of EMR systems on the structure of healthcare delivery systems. That means that EMR systems should be mandated to be completely open, but with standards to assure that all EMR systems can collate and integrate EMR from any other system. The selection of an EMR system should not lock any provider into working only with other providers which have the same EMR system.

Finally, more work needs to be done on addressing the privacy issues associated with making EMR records broadly available to any other provider treating the patient. There is a clear trade-off between broad access and privacy. Care must be taken to not err on the side of privacy constraints to the point of impeding the development of an EMR system

that provides full access to the complete medical record of a patient by every provider treating the patient.