TEXAS MEDICAL ASSOCIATION

Physicians Caring for Texans

February 15, 2017

The Honorable Kevin Brady
1011 Longworth House Office Building
Washington, DC 20515

Dear Congressman Brady:

As our state's premier health care organization, representing more than 50,000 member physicians and medical students, the Texas Medical Association appreciates your interest in better understanding how to improve electronic health information exchange (HIE). Billions of dollars spent through the HITECH Act's Electronic Health Record (EHR) Incentive Program have successfully increased adoption of EHRs such that most physicians now use them. Some physicians have found ways to leverage their EHR to improve quality and decrease costs of care in their individual practices. Nevertheless, the expectation that EHR adoption would *transform* health care has failed to materialize, and this is primarily because most patient health information is still "locked" inside the physician's office; only today it is in their EHR rather than in a paper chart. The principal function of HIE is to unlock the *transforming potential* of EHRs by allowing patients (and their physicians) to electronically, securely, and confidentially share their EHR data with any other physicians and health care facilities they trust. So, although the HITECH Act has increased adoption of EHRs, the potential for EHRs to *transform* health care remains constrained by the lack of effective HIE.

The main technical constraint to effective HIE is that vendors use proprietary systems that require *interfaces* and *custom data mapping* to transfer data and make them easily available for use. This is often referred to as a lack of EHR "interoperability." The main non-technical limitation is a concern over data security and liability. Each of these is discussed in more detail below.

Interfaces and Custom Data Mapping

The first part of the interoperability problem regards the actual movement of data between systems (i.e., an interface). Interfaces typically are done through:

- Connecting multiple EHRs to a single health information exchange organization (e.g., the Houston or San Antonio HIE);
- Making a direct connection between the computers of two organizations without an HIE (e.g., a laboratory interface to a hospital);
- Sending information one episode at a time through secure email (e.g., the DIRECT system);
- Retrieving single pieces of information through a special query (e.g., using the Fast Healthcare Interoperability Resources (FHIR) standard, which is in development and can be useful in some cases where specific information is needed); or

- Using the “Blue Button” or the equivalent to provide patients a copy of their own data and allowing them to provide it to the next physician/care location. This is rare and sometimes is supported by an HIE or by using the DIRECT email system.

Each of these has advantages and disadvantages that we would be happy to explain in more detail, but at least in the near term, all five need to exist. Encouraging the last approach (patient-mediated transfer) probably increases patients’ responsibility and understanding of their health information, so it may offer the most overall value in the long run.

The second part of the interoperability problem is data mapping. Mapping is needed so the transferred data can be used by the receiving EHR/system rather than just viewed. For example, if a patient has a problem identified as “Type II diabetes,” a simple interface can move this text to another system where it can be viewed. However, to be useful in automated alerts and care planning, mapping must translate this information so that it has the same “meaning” in the receiving system. To create the appropriate meaning, the “Type II diabetes” text typically must be put into the correct part of the receiving EHR’s database so that EHR “knows” the patient has this type of diabetes. While this example may seem simple, the proprietary nature of EHRs makes this difficult even with the increased use of standard codes.

Mapping isn’t always possible between systems because of differences in the clinical models that they use. For example, some EHRs differentiate between allergies (e.g., penicillin) and intolerances (e.g., stomach irritation with aspirin), which is appropriate. However, others do not make this distinction and so the aspirin intolerance becomes an aspirin allergy when the data is moved to the other EHR.

Additionally, because of the way EHRs typically are designed and implemented and the mapping required, vendors frequently claim that the programming needed to map the data from one of their customers to an HIE or another system cannot be used to connect another customer using the same EHR and same HIE. Thus often there are few economies of scale.

Unfortunately, once the initial interfaces and mapping are done, the costs don’t stop. With computer-to-computer connections, every time upgrades occur in any of the now-connected systems, testing and possible rework must follow because of incompatible changes, often at significant expense and increased risks to patient safety. These types of interfaces also require frequent or continuous monitoring. Even simple secure email (e.g., DIRECT) can require some degree of ongoing testing and monitoring as changes can occur that break the communication chain.

The negative effect of custom interfacing and mapping goes beyond simply transferring meaningful data for continuity of care. For example:

- When a physician/hospital needs to move from one EHR to another, e.g., if a vendor performs poorly or goes out of business, the cost to transfer data usually is prohibitive. This makes physicians reluctant to change EHRs, even if theirs is poorly designed. Physicians/hospitals often will remain with an inferior product simply because there is no cost-effective way to move a complete patient record for thousands of patients in a short time at low cost.

- When physicians/hospitals do make the transfer to a new EHR, important patient data is almost always lost. It is probably only a matter of time before this problem causes a serious adverse event. For example, TMA knows of cases where patient allergies were not transferred in EHR changes.
- When a physician plans to retire and close his or her practice, he or she has a responsibility to maintain patient records for a period determined by state medical boards. In Texas, this ranges from seven years for an adult patient to more than 21 years for a child. The technical expertise and expense required for long-term maintenance and access of electronic records are arduous and costly. In many cases, the data simply may not be available because the expense of making it available is too great.

Back in 2009, vendors and the federal government could have worked together to standardize interfaces and data mapping so that interoperability would be a natural byproduct of EHR use. Sadly, they failed to do this for a variety of reasons.

However, there is still a chance to make things better.

For many years, TMA has advocated for universal use of extensible markup language (XML) or a similar standard (e.g., FHIR) as a way of exchanging meaningful health data. Universal common XML encoding of *all* data could permit disparate systems to share and consume information much more easily. Information consumed by a receiving EHR could be placed correctly within the system to give it meaning and make it useful.

A simple example that is not currently possible is transmitting pacemaker information and settings between a hospital and the follow-up physician's EHR, even in some cases if they use the same vendor. XML coding (or a similar standard) could make this easy and cheap. This would allow the information in the receiving EHR to be searchable, extracted for reports (such as medication or device recalls), and available for clinical decision support.

A more complex example of the benefits of standard tagging in an EHR database is where a physician desires to change EHRs. If the receiving EHR has the same functionality as the sending EHR (as described in the allergies versus intolerances example above), standard tagging would make it possible to move from one EHR to another almost instantaneously and at little to no cost.

XML is the approach used by the accounting industry to exchange financial information very successfully and cheaply. XBRL (eXtensible Business Reporting Language) is a free and "open" XML standard for tagging business and financial data. It is maintained by XBRL International, an international nonprofit consortium of approximately 450 major companies, organizations, and government agencies around the world.[1]

FHIR is a developing standard and could also be used for health care tagging where standards exist.

The most important part of gaining the benefits of tagging is that there is universal acceptance and adoption. For a variety of reasons, in health care vendors and the federal government have become

[1] See www.fasb.org/jsp/FASB/Page/SectionPage&cid=1176157087972 for more information.

dominant, and to date they have failed to get us where we need to be. TMA strongly recommends a private standards-setting body with disciplinary teeth in which physicians and clinicians are full partners.

Data Security and Liability

Even if all of the technical issues of interfaces and mapping were solved through the use of standard data tagging, the issues of concerns over data security and liability loom large.

Physicians are concerned about the security of health information exchange and need protections to avoid being inappropriately penalized or held financially liable for breaches and other problems that are inherent with electronic data exchange between health care entities. In particular, MACRA (Medicare Access and CHIP Reauthorization Act), requires that physicians must attest that they did not block the sharing of patient information, regardless of the level of maturity of systems to which they connect. This could put physicians at risk for substantial liability if a significant data breach occurred beyond their control, not to mention the real harm that could occur to patient care and patient privacy. Some of the many additional costs would include hiring a privacy attorney, establishing a call center, providing credit-monitoring/theft-restoration services, and loss of income due to reputational harm. All of this is because of actions beyond the physician's control.

TMA supports a focus on the maturation of HIE processes and reduction of its security risks.

Finally, physicians are concerned about being deluged with data and being held liable for having received data that it is impossible to review. The risk of not seeing an important piece of information about a patient is significantly higher with EHR transfers than with paper, largely because of differences in volume.

TMA is happy to work with you to develop proposed legislation to address these issues. Until they are addressed, TMA feels it is not appropriate to penalize physicians who do not participate in health information exchange because of these concerns.

* * *

Following this letter is an addendum that provides TMA's HIE Guiding Principles. We adopted these almost 10 years ago, and they remain important today. We offer them to help with your understanding of the complexity of interoperability beyond the technical aspects described here.

TMA is eager to assist you and others in resolving these interoperability problems for the benefit of physicians and other clinicians. More importantly, TMA wants to get this working for better and safer care for the patients whom we serve.

Sincerely,

Matt Murray

Matt Murray, MD
Chair, Ad Hoc Committee on Health Information Technology
Texas Medical Association

Addendum
Texas Medical Association Health Information Exchange Guiding Principles
Adopted 05/01/2010

1. Core Principles

- Patient safety, privacy, and quality of care must be the guiding principles of all health information exchange efforts. Cost reduction and efficiency should be expected byproducts.

- Patients have the right to their medical records, but some parts of their medical records (e.g., diagnoses) should be considered the intellectual property of the physician. Health information exchange efforts should recognize that the physician's work product has value for which he or she, along with the patient, has intrinsic ownership, and therefore both should control its use.

- Health information exchange efforts must be designed to engage patients, transform care delivery, and improve population health. Patients/individuals and physicians must have confidence that personal health information is reliable, private, secure, and used with patient consent in appropriate, beneficial ways for patient and public good.

2. Special Patient Privacy and Confidentiality Considerations

- Patient privacy protections that traditionally exist in the patient-physician relationship continue to apply where health information technology is utilized. Physicians must uphold their responsibility to protect and secure all information related to this sacred relationship.

- Patients have the right to withhold information. A notice to users that the record is incomplete may be provided when information is withheld from transmissions.

- Patient privacy and confidentiality must be maintained in all health information exchange efforts by using secure systems and transmission methods.

- Patients/individuals should have complete control over all uses of individually identified medical data. Except for emergencies, or otherwise as required by law, their medical data should not be disclosed or disseminated to third parties without their agreement.

- Participation in health information exchange efforts should be the default. Participants should be able to withdraw upon reasonable notice.

- To facilitate HIE, patient consent forms used by organizations providing patient care must specify — using clear standard language nationally — that the patient's data will be transferred within 12 hours to a nonaffiliated organization upon discharge or completion of the immediate patient care event. Participation in an independent HIE or transfer of the patient's data to their independent personal health record can satisfy this requirement.

- Each organization exchanging health information must define how and whether it will share information for public health research and surveillance and evaluation of health care quality.

When it chooses to allow these uses, it must require that patient information be deidentified unless documented informed consent has been obtained.

- The integrity of patient/individual identification is critical to successful health information exchange. Techniques that support appropriate matching (e.g., biometrics, voluntary identifiers, etc.) of existing and new information should be used. The Social Security number must not be used as the unique patient identifier.

3. Standards and Data Integrity

   - Standards used for health information exchange should be acceptable to the medical community and compatible with national and regional standards.

   - Health information exchanged must not lose or change its original meaning or emphasis as it is exchanged. Wherever possible, health information exchange operations should not modify original patient data in any way.

   - Provenance (the source) of data must be maintained and available without significant effort whenever data is exchanged.

   - Health information exchange must provide timely, relevant, and actionable data as a discrete part of the physician's electronic workflow at the point of care. "Actionable" means that data reconciliation and data integration can be performed by a competent individual so that it is available for automated clinical decision support in the physician's electronic system.

   - Standards and processes should be developed that support:

     - "Push" systems that notify clinicians of the availability of patient's new information rather than "pull" systems requiring the clinicians' action to search for data.
     - Systems that distinguish new information from that which is already known.
     - The ability of physicians to move their data between systems without incurring significant delays or costs. The concept of a clearinghouse financially supported by all health information exchange vendors that supports this exchange should be investigated.

   - Patient data must be transmitted over secure networks and encrypted. Standard email services do not meet this requirement.

   - Organizations providing health information exchange must be aware of security risks and guard against them using technology, individual training, and frequent assessment/monitoring. They must have a means to audit, track, and use reasonable efforts to ensure the integrity of all entities or individuals engaged in managing data.

4. Costs of providing health information exchange should be clearly defined, fair, simple to understand, and borne by all stakeholders, and should support the financial viability of the clinical practices that generate and consume health information.

5. Governance/Leadership of Organizations Providing HIE

    - Governance/leadership of organizations managing health information must be representative of and responsive to the needs and concerns of stakeholders, with particular attention to the concerns of physicians and patients. Consideration should be given to special populations who are otherwise incapable of representing themselves (children, disabled, uninsured, homeless, aged, etc.).

    - Strictly enforced policies must require disclose of conflicts of interest and recusal from deliberations and/or voting where there is such a conflict.

    - Financial transparency of intermediary organizations in health information exchange must be conducted.

    - State and federal support for health information exchange is important. However, government’s primary role should be to foster coordination of health information exchange efforts, including providing access to funding or other financial incentives that promote the adoption of health information technologies.

6. Enforcement

    - An independent National Health IT Safety Center should be formed to conduct enforcement of any statutes related to safety, which includes interoperability.

    - Complaints about vendors who produce systems that are alleged to not be compliant with interoperability requirements should be investigated by this Center and treated as they are potential safety events.

    - If vendors are found to be noncompliant, all product information must contain a black box warning that the product can cause harm if used. The black box can be removed only after the Center clears the compliance issue.