

Sharing an EHR Application Across Multiple Organizations

Save to myBoK

By Lori L. Richter, MA, RHIA, CPHIT, CPEHR, CHPS

Regulatory developments in the healthcare industry, including the Health Information Technology for Economic and Clinical Health (HITECH) Act, accountable care organization provisions, and the “meaningful use” Electronic Health Record (EHR) Incentive Program, have contributed to a recent boom in health information technology (IT) development and adoption. In particular many providers have begun exploring and implementing EHR systems and strategies, including integrated EHRs which allow two separate provider organizations to use the same EHR system as well as share records for the patients they have in common.

While there are benefits for organizations that embrace an integrated EHR system, there are many factors to carefully consider before implementing an integrated EHR environment. This includes fully understanding which records (medical, billing, etc.) the integrated EHR environment will encompass as well as how these records can later be extracted in the event one of the participating organizations chooses to end their involvement in the integrated EHR environment.

Considerations include the configuration and type of technology involved, security requirements, regulatory influences, and the type of relationship between the organizations. Furthermore, the organizations need to clearly outline how the business processes will be maintained in regard to operational management of the records, such as responding to requests for patient corrections or amendments and management and maintenance of the master patient index. These records are considered business records for the organizations involved.

Integrated EHR systems are only appropriate from a legal compliance perspective if certain affiliations or relationships between the involved organizations exist. The integrated EHR relationship should include legal contracting, along with a clear understanding of what will happen in the event a participating organization needs to divest from the relationship. The relationship should be clearly documented, including the intention for each organization’s integrated operation and the legal and operational reasoning for the arrangement.

Access to one organization’s information through an integrated EHR system by another organization is viewed as a “disclosure” by the data source provider, and this disclosure must meet a pertinent HIPAA Privacy Rule exception for disclosures without patient authorization. Additional regulatory considerations need to be thoroughly vetted as well, such as requirements for maintaining the confidentiality and integrity of medical records under federal regulation 42 CFR§482.24(b)(3).

Leading the Effort with a Multidisciplinary Team

A multidisciplinary team comprised of leaders from health information management, clinical information technology, information technology services, privacy, security, legal, and corporate responsibility should be put together to create a scope document. The scope document should help the team outline their goal and deliverables, listing constraints, assumptions, and facts. This document is a tool that should be utilized by all participating organizations to ensure compliance with regulations; and the document should clearly define what is best for the organizations and their patients.

In addition, this team must evaluate the technical structure of the EHR. When discussing an integrated EHR system, the planning must clearly outline how the EHR system will display patient records (or the data elements) for user access across each of the organizations.

To determine whether an appropriate relationship exists for the implementation of any EHR, including implementation that creates an integrated EHR environment, one of the following criteria must be met:

- The organizations are the same legal covered entity or share the same tax ID

- The entities are affiliated under the same legal ownership; if so, then consider whether such entities are within the same region or treat the same patient population in which the surveyors/reviewers would expect collaboration in patient care
- The organizations are part of an Organized Health Care Arrangement (OHCA)
- The organizations all participate in the same clinically integrated network or accountable care organization, or the organizations legally outline a shared operational intention for integration
- The entities have a joint operating relationship where the organization that maintains/hosts the EHR system is the managing partner, and the contract outlines shared collaboration and management of the integrated medical records

If a relationship meets any of the criteria listed, then an integrated EHR system may be appropriate. The relationship is still dependent on whether the technical structure of the EHR system and the organizational policies support all regulatory requirements. If a relationship does not meet any of the circumstances listed above, then it is not appropriate for the organizations to pursue participation in an integrated EHR environment.

Regulatory, Legal Factors to Consider

There are numerous regulatory and legal considerations that impact these types of relationships. In an integrated EHR system, it is recommended that each participating organization inform its patients of the data sharing arrangement. An appropriate means for notifying patients of such an arrangement is through each organization's Notice of Privacy Practices.

An integrated EHR increases the risk for potential liability for the hosting organization. A greater amount of clinical information will be available in an integrated EHR environment, which in turn brings the potential for increased malpractice liability related to failure to access all available information. In order to mitigate this risk, organizations should provide thorough physician training on how to use all the tools available in the EHR system. Organizations participating in an integrated EHR should work with their risk and insurance staff to review their malpractice and cybersecurity insurance options.

Ultimately, whether an organization participates in an integrated EHR environment or employs a non-integrated EHR, they must effectively manage their legal health record with clear intentions to ensure the integrity of all data, records, and information. Medical records are not only an important tool for supporting patient care decisions, but are also integral in validating the revenue cycle and can serve as the organizations' business and legal record.

References

AHIMA. "[Fundamentals of the Legal Health Record and Designated Record Set](#)." *Journal of AHIMA* 82, no. 2 (February 2011); expanded online version.

Department of Health and Human Services. "[42 CFR Part 482. Medicare and Medicaid Programs; Hospital Conditions of Participation: Patients' Rights; Final Rule](#)." *Federal Register* 71, no. 236 (December 8, 2006).

Department of Health and Human Services. "[Confidentiality of Substance Use Disorder Patient Records \(42 C.F.R. Part 2\)](#)." *Federal Register* 82, no. 11 (January 18, 2017).

Department of Health and Human Services. "[Summary of the HIPAA Security Rule](#)."

Office of Inspector General. "[A Roadmap for New Physicians: Fraud and Abuse Laws](#)."

Office of the National Coordinator for Health IT. "[Guide to Privacy and Security of Electronic Health Information](#)."

Lori L. Richter (loririchter@catholichealth.net) is the national director for EHR compliance in the corporate responsibility department at Catholic Health Initiatives.

Article citation:

Richter, Lori L. "Sharing an EHR Application Across Multiple Organizations" *Journal of AHIMA* 88, no.10 (October 2017): 52-53.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.