Information Governance Initiatives Essential for Strategic Alliances

Save to myBoK

By Melinda Patten, MHA, RHIA, CHPS, CDIP; Karen Proffitt, MHIM, RHIA, CHP; and Susan Lucci, RHIA, CHPS, CHDS, AHDI-F

IN TODAY'S HEALTHCARE reform landscape, collaboration and care coordination have emerged as key pillars in the quest to improve the cost, quality, and access to healthcare in the US. As a result, organizations across the nation are entering formal and informal alliances designed to broaden reach and successfully participate in shared-risk care/reimbursement models under current reform legislation.

Included in these alliances are health information exchange organizations (HIOs), hospital-within-hospital, application service provider (ASP), and electronic health record (EHR) hosting initiatives, to name a few. Yet while the form of alliance or affiliation may vary, the goal is ultimately the same—to improve the quality of care provided to the communities served.

Doing so is not without its challenges, particularly to ensuring the integrity, privacy, and security of patient information. Collaboration between healthcare organizations requires the exchange of comprehensive patient data across otherwise unaffiliated organizations, meaning organizations must coordinate information exchange while also ensuring compliance with the Health Insurance Portability and Accountability Act (HIPAA) and preventing intentional and unintentional breaches of protected health information (PHI).

Information Governance Key to Alliances

To effectively address privacy and security within an alliance, it is first necessary to establish a framework for data sharing and information governance. Doing so across multiple healthcare organizations often comes with its own set of challenges.

For instance, each participating organization will have its own medical staff bylaws and procedures in place. Affiliation leaders must take into consideration the differences in these and determine which processes will prevail. To avoid confusion, communication of these decisions must be routinely shared with key stakeholders.

Current data management processes must also be examined to identify any differences that may potentially impact the success of the alliance. This includes data capture processes and naming conventions, as both play an important role in ensuring data integrity and avoiding the creation of duplicate and overlaid records.

HIPAA Compliance Factors

Sharing key patient care data takes place routinely within affiliated organizations to carry out treatment and operational business. In addition, affiliated organizations may require the exchange of comprehensive patient data across multiple unassociated organizations. Compliance with HIPAA and other privacy and security regulations can be the most significant governance challenge alliances face. In addition to accounting of disclosures, minimum necessary, and audit trails, governance policies for alliances must enable data access and usage across multiple institutions that is secure and HIPAA compliant.

Collaboration on policies to address consistency in different organization's Notice of Privacy Practices and to facilitate coordination of requests for restrictions across all facilities is vital. It is also crucial to consider varying state laws when facilities are located in multiple states, including those pertaining to emancipated minors, PHI, and release of information regulations.

Establish an Information Governance Framework

The first step in establishing a strong governance framework to help guide an affiliation is the appointment of a multidisciplinary team representing both the clinical and business interests of stakeholders. This should include—but is not limited to—individuals from health information management (HIM), information technology (IT), case management, quality, compliance, and privacy and security.

Once established this team should examine the various frameworks in place at affiliate organizations and determine which policies will remain and which will be replaced by stronger, more effective practices. Armed with this information, key stakeholders can begin drafting a unique governance framework that will be put in place across the various affiliate organizations.

Included in this should be standards and best practices for the design and capture of information, as well as the quality and integrity of data exchanged. The alliance must also determine what data will be shared, who can access it and for what purposes, and how it will be distributed across the organizations (i.e., through interfaces or portals).

Break-the-glass system functionality must be considered as well in the event of an emergency so providers can quickly access information, and procedural implications need to be addressed. It is important that role-based access be consistent across the affiliation continuum to ensure alliance partners meet the HIPAA minimum necessary requirements.

Guidelines should define how information is collected, accessed, managed, who is responsible for maintaining data quality and integrity, and who is responsible for driving decisions and achieving consensus to keep the alliance intact. To that end, processes should be set in place to monitor and regularly communicate progress between the participating organizations. Documenting decisions and accomplishments for recordkeeping and process improvement purposes is recommended.

While this framework should start with EHR-centric guidelines, it must also have the flexibility to expand and take into account a number of operational considerations to support data integrity and exchange. These include master patient index (MPI) integrity; release of information; coding and billing; transcription; performance indicators/measures; meaningful use; discrete data loss; audit reconciliation; reporting; consent management; and resource allocation.

A properly designed framework will minimize the impact of participating in the alliance on individual facilities. By aligning pertinent policies and procedures and informing all staff, management, and key stakeholders, organizations create accountability and establish a baseline for success. Engaging HIM at all stages of the process will ensure that the appropriate resources are set in place to successfully share information across the organization.

Governance in Action: CHCO and UC Health

For Children's Hospital Colorado (CHCO) and the University of Colorado Health System (UC Health), addressing the privacy and security challenges inherent to strategic alliances became a focal point in October 2012 when the two organizations formed a collaborative entity to enhance the quality of care and treatment provided to children in the state of Colorado. This move was a natural extension of an alliance between University of Colorado Hospital and CHCO that had been in existence for several years, driven in part by the close proximity of the two health systems and later the acquisition of Memorial Health System (MHS) by UC Health.

The initial alliance between CHCO and UC Health occurred when the former assumed the 105 pediatric acute-care beds at MHS, creating a hospital-within-a-hospital. Later on, UC Health decided to transition its entire system to an EHR that would be consistent throughout all its hospitals and clinics, including MHS. By association, CHCO at MHS would also transition to this new EHR. The EHR vendor was the same being used at CHCO hospitals and clinics.

However, the system versions were different. Although their original system integration only included an admission-discharge-transfer (ADT) feed, this evolving transition found CHCO hosted on MHS's EHR, sharing their master patient indices (MPI), registration, scheduling, and clinical documentation systems. CHCO now shares many of the policies and procedures governed by MHS.

Challenges and opportunities have been plentiful. For example, the decision to assure all patient information for children treated by CHCO at MHS would be "whole" in CHCO's electronic patient record requires duplication of registration, scanning large amounts of documentation, and a PDF electronic transfer of most of the clinical information. Making the record whole was one of the most challenging efforts for the HIM department. CHCO has taken on many additional functions requiring hiring

and training additional staff to manage the workflow processes for health information maintenance and to assure timely coding and billing.

In preparation for the transition, UC Health, MHS, and CHCO needed to ensure that all common patients across their three MPIs were linked at an enterprise level. It was also imperative that each respective site resolved as many duplicate records as possible prior to sharing MPIs. To accomplish this huge project in an accelerated time frame, CHCO engaged a leading data integrity vendor to help identify any duplicates between the MPIs. It was imperative to ensure that all possible duplicates were resolved prior to sharing MPIs. From a privacy standpoint, it was also critical that each patient visit clearly reveal which entity was the "owner" of that visit to avoid inappropriate PHI disclosures.

By properly addressing HIPAA compliance as well as privacy and security from the outset with well-defined information governance policies and procedures, CHCO and UC Health are now reaping the benefits of strategically sharing information, technology, and responsibilities—all while ensuring patient privacy and confidentiality.

Melinda Patten (Melinda.Patten@childrenscolorado.org) is director of HIM at Children's Hospital Colorado. Karen Proffitt (kproffitt@justassociates.com) is vice president of consulting services and Susan Lucci (slucci@justassociates.com) is consultant and chief privacy officer at Just Associates.

Article citation:
Patten, Melinda; Profitt, Karen; Lucci, Susan. "Information Governance Initiatives Essential for Strategic Alliances" *Journal of AHIMA* 85, no.4 (April 2014): 48-49.