HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

July 2015

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Congratulations, Laura!

an interview with Laura Burke — our 15,000th member

See page 18

by Janice Anderson and Ken Briggs

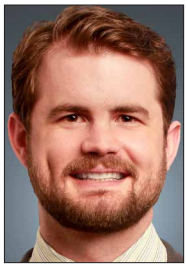
Creating effective solutions for data privacy concerns in clinically integrated networks

» Clinically integrated networks are becoming the cornerstone of the healthcare delivery system.
» Privacy laws pose complex and contradictory hurdles for successful integration.
» Data exchange through networks has significant liability and regulatory implications.
» Certain structures of clinically integrated networks are more effective than others.
» Networks should investigate different options to structure the network in light of applicable state and federal privacy laws to determine the most efficient solution.

Janice Anderson *(janderson@polsinelli.com) is a Shareholder in the Chicago office and* ***Ken Briggs*** *(kbriggs@polsinelli.com) is an Associate in the Phoenix office of Polsinelli PC.*

The healthcare system is transitioning from one that ties payment to the quantity of services rendered to one that ties payment to quality. One milestone of progress, described by the Secretary of Health and Human Services on January 26, 2015, is the goal that by 2018, half of all Medicare payments are projected to be tied to the quality of the services provided.[1] One way to achieve this goal is through payment models that require the use of clinically integrated networks or accountable care organizations (ACOs). These organizations establish new ways for providers to work together to enhance the quality of services across the healthcare spectrum. Data—derived from patient information—is the fuel for these new delivery systems. Patient information also provides the measure for how well the services are being provided, and as a result, is the basis for how providers are compensated in these new delivery systems.


Anderson


Briggs

Laws that impact how providers may use and disclose patient information in the context of these new delivery systems have not kept up with changes to how care is delivered. Specifically, healthcare is being provided increasingly through clinically integrated delivery systems, which require the sharing of patient information in ways that are different from the past. These networks of providers need to be carefully structured to efficiently navigate privacy laws, and each structure may be different depending on the network's purpose, the interests of the participants, and applicable state and federal privacy laws. This article will provide an outline of modern delivery systems, discuss the impact of state and federal data privacy laws, and highlight trends of how networks are being structured to address privacy requirements.

Successful networks and the exchange of information

Providers can work together in a number of ways. Integrated networks of providers are

usually composed of legally separate providers, many of which render different types of services. Networks include those built around achieving quality metrics (such as lowering readmissions) or enhancing the flow of information among local providers who treat the same patients. Accountable care organizations, physician hospital organizations, and independent practice associations are examples of structures that may become clinically integrated networks.

The basic structure of a network involves a "hub" or central entity, whether it is a separate administrative entity or a participant in the network, that enters into contracts with providers to secure participation in the network. Almost any type of provider can participate in a network, including most commonly individual physicians, physician groups, and hospitals. The central entity usually performs management and administrative services for the network, such as engaging vendors, contracting with payors, and analyzing data that flows through the network to assess and improve the quality and efficiency of care.

To achieve their purpose of improving quality or providing services more efficiently, networks must invest in infrastructure to share information, which may be achieved by creating a health information exchange, joining a separate exchange, or by sharing the same system. These information systems make the transfer of data between providers easier, both in terms of technological advantages and sharing the costs of infrastructure improvements among providers. Because of the infrastructure, time, and costs involved in developing the systems, decisions regarding information exchange should be a principle consideration when structuring the network.

Health information exchanges can be formed privately among participants, through a regional exchange, or through a national public exchange. Typically, these exchanges have separate technologies that connect to the electronic health records (EHR) systems used by individual participants. The patient information can be transmitted through the exchanges in different ways, as needed by the network. For example, an exchange may be set up to allow participants to send data to another participant directly (a directed exchange) or to request data from another participant (a query-based exchange).

Providers that are closely integrated are moving towards sharing the same system of health records. This "shared medical record" arrangement means that one system maintains the entire record of the patient; there is no exchange of information.

Providers that are closely integrated are moving towards sharing the same system of health records. This "shared medical record" arrangement means that one system maintains the entire record of the patient; there is no exchange of information. These shared systems promote the most integrated arrangement, and as a result, require the most operational adjustments to use one system.

Efficient exchange of information is essential for clinically integrated networks to use the data to shape practices and outcomes of the network. Once the technology and ideal method of sharing information is established, the privacy laws must be analyzed to determine appropriate safeguards.

The obstacle of data privacy laws

State and federal laws impose different and sometimes conflicting obligations on how data may be used in modern healthcare arrangements. Legal obligations may affect how the network participants document their arrangement, communicate with patients, and use or disclose information among participants.

Most, if not all, states have enacted laws that impact the flow of information among providers, and most state laws apply even to information exchange in integrated arrangements. States impose requirements, conditions, or limitations on how information is shared through statute or regulation. Medical information is regulated by states in a combination of ways:

- States may have a defined series of statutes that regulate all medical information.
- The use or disclosure of medical information may be restricted through licensing requirements according to the type of provider. For example, states may impose additional or different patient privacy requirements on a hospital, but not a physician.
- States may impose requirements on specific types of medical information (e.g., communicable diseases, mental illness, substance abuse).
- States may impose specific data privacy obligations on specific arrangements, such as health information organizations.

The entire body of a state's regulation of medical information should be scrutinized to identify how each of the participants and the network can maintain compliance with these regulations in a new delivery system.

The federal government imposes restrictions on the use or disclosure of patient information primarily through the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The regulations of the HIPAA Privacy and Security Rules are set forth in 45 C.F.R. Parts 160 and 164. HIPAA regulates the use and disclosure of patient information through the Privacy Rule and imposes safeguards and protections on electronic patient information through the Security Rule.

HIPAA applies to covered entities and business associates. Covered entities include health plans and healthcare providers; business associates are entities that perform services for or on behalf of covered entities. HIPAA affects integrated provider networks in two important ways. First, the law requires entities subject to HIPAA to implement technical, physical, and administrative safeguards to protect the storage and transmission of patient information. These safeguards must take into account the provider's participation in the network and the services provided between them. Second, HIPAA imposes restrictions on how providers may use and disclose information throughout the network, depending on how the network is structured.

In addition to HIPAA obligations, federal law also restricts the ability of substance abuse treatment providers to share information, even in the context of integrated care. The substance abuse privacy regulations (at 42 C.F.R. Part 2) extend to other participants in a network when substance abuse information is shared. These regulations, enforced by criminal penalties, require even higher standards, safeguards, and protections applicable to substance abuse records. Industry stakeholders have called into question the efficacy of the regulations and the government has been considering modifications. Regardless of how these regulations are revised, all of the participants in a network should be aware that sharing substance abuse information protected by Part 2 is restricted by federal law.

Networks and their participants must comply with HIPAA where it conflicts with state law, unless the state law provides a greater right of privacy or a greater right of access to

the patient. The privacy laws adopted by states may not be consistent with HIPAA, which sometimes results in a patchwork of obligations that relate to the same conduct. Access, opt-out, and consent protections are categories of state regulations that are most often more stringent than HIPAA. States may also, however, enact requirements necessitating specific communications to patients, obligating the network to maintain information in a certain way, or requiring the network to develop and follow specific policies. Where these state laws offer greater privacy or access rights than HIPAA, networks must operationalize these obligations through network policies and sometimes in individual participant policies. These obligations also must be observed in the network's technology. For example, the data sharing systems must permit certain information to be sequestered or blocked before it gets to the network. The technologies should also be able to indicate when consents are required or obtained, and trigger and document communications provided to the patient.

In addition to how participants may use and disclose information, most states and HIPAA have adopted regulations describing minimum standards for safeguarding patient information or for performing certain notification obligations in the event of a breach of patient information. These breaches often trigger obligations to notify the patient, state and federal governments, the media, and even consumer protection agencies—all within specific deadlines. Network participants must consider the exposure to liability resulting from non-compliance with laws or uses or disclosures not permitted by the laws. These liabilities—and the obligations triggered by the liabilities—should be considered when the network is organized.

Participants should understand how these obligations apply to the other participants in addition to their own obligations, because entering into a contractual relationship with other entities could expose the participant to new obligations. Given that networks are cutting-edge arrangements, breaches of information pertaining to a network can be very complex to investigate and resolve. Although some breaches may be relatively straightforward, such as a lost portable device, other breaches involving a network may be more complex and involve more than one participant.

Participants should understand how these obligations apply to the other participants in addition to their own obligations…

Trends in efficiently navigating patient privacy laws

Networks that have succeeded in bringing participants together in a way to achieve effective integration share the motivation to deal with data privacy laws from the beginning. Networks should consider how to address patient rights that may be protected by law and relate to providing patients a chance to opt out of data sharing through an exchange or a right to consent to the use of an exchange for sharing certain information throughout the network. These laws need to be identified at the outset of the arrangement to ensure that the participants are aware of their responsibilities to discuss the rights with the patient and to secure any required authorizations. The ability of the exchange software to sequester, block, flag, or remove information from the network should be specifically verified with the vendor to ensure that the software can accommodate patient rights or requests. If a patient with a

right to opt out does not wish to be included, or if certain information is subject to consent requirements prior to release, the software should be able to accommodate these issues without fail.

In addition to the patient rights, the way in which network participants document their relationship and hold themselves out to the public as participating in a network will affect how privacy regulations apply to the network. A network may be able to achieve greater flexibility for the exchange of patient information, however, by organizing itself as an organized healthcare arrangement (OHCA) under HIPAA.[2] Structuring the network as an OHCA permits network participants to exchange information more easily and may provide additional protection in the event of a breach of information. To properly organize the network as an OHCA, the participants must hold themselves out to the public as participating in a joint arrangement and participate in utilization review, quality assessment, and improvement activities, or payment activities where the financial risk is shared among the participants.

An OHCA can include only covered entities. Therefore, the network, along with other entities performing services for the network, would still need to enter into business associate agreements with the OHCA.[3] Participants involved in an OHCA should describe their participation in the OHCA and the permissible exchanges of information through the OHCA in each participant's Notice of Privacy Practices.

Agreeing to the security standards and privacy practices of participants in a network is essential, given the enforcement environment. The obligations of the parties as to how they may use and disclose patient information, and the minimum safeguards maintained by each of the participants, must be dictated through contract. The poor practices of one participant can lead to an impermissible use or disclosure of patient information across multiple, if not all, participants. "[I]f the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate."[4]

The security of the network is only as strong as its weakest link. A serious breach of patient information can damage any provider relationship and, with the size of modern breaches, can cripple a network. Given the significant risk, the parties should dedicate serious effort to agreeing on the minimum security standards required of participants, and the expectations for the parties to discover, investigate, and report breaches of patient information. These expectations should be detailed in network documents and should be consistent with any ancillary agreements, including participation in a health information exchange and business associate agreements. In discussing these obligations, the participants should consider how to determine reimbursement for costs involved in the breach (including third-party consultants and costs to notify the patients) and how to allocate damages resulting from a breach.

Conclusion

Successful networks have achieved that success by establishing the purpose and the trajectory of the network into the future, identifying the legal obligations of the network and each participant, and delineating the obligations and expectations in the network documents. Once this investment is completed, the networks can determine ways to navigate successfully through the obstacles of the data privacy laws and focus on delivering quality care.

1. Sylvia M. Burwell: "Setting Value-Based Payment Goals — HHS Efforts to Improve U.S. Health Care." *The New England Journal of Medicine,* January 26, 2015. Available at http://bit.ly/1Ehm5dQ (paywall)
2. 45 C.F.R. § 160.103.
3. 45 C.F.R. § 164.502(e).
4. *See* 45 C.F.R. § 160.402.