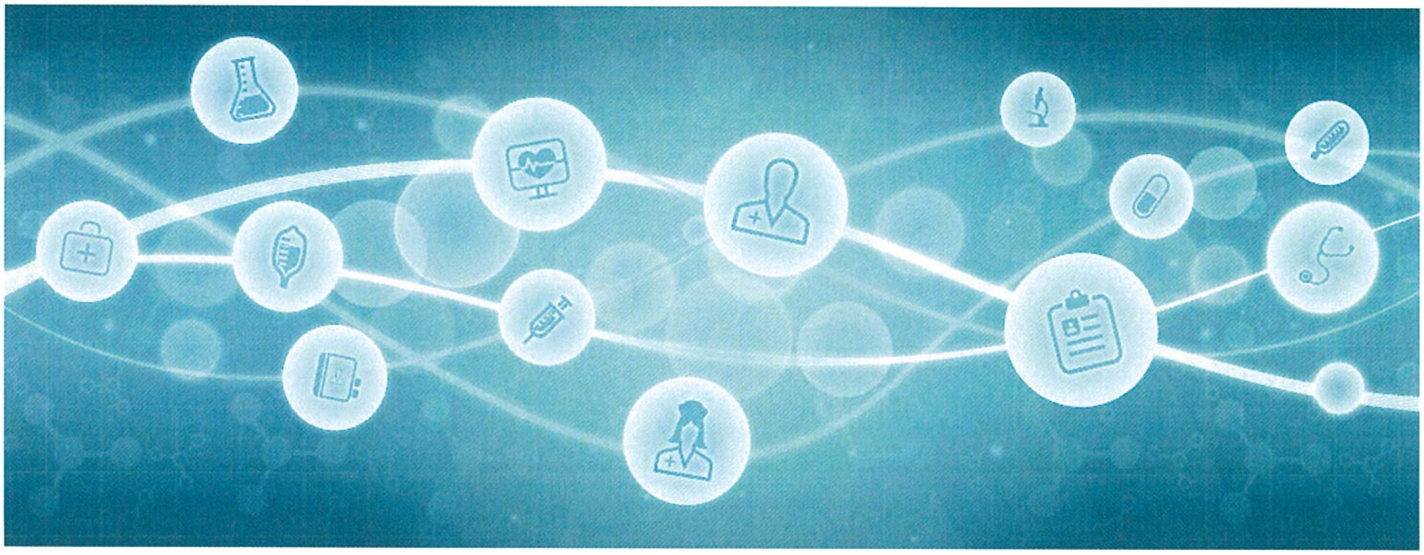

The Intersection of Health Information Exchange and Patient Confidentiality

by Deborah A. Cmielewski

Almost everyone has a friend or relative who suffers from a chronic condition requiring ongoing medical treatment and consultation with multiple providers. These patients maintain copies of their medical records, laboratory results and films, toting them back and forth to various appointments. Depending upon the patient's condition, there may be volumes of materials housed in boxes, binders or briefcases; these records are not always secure, and they are frequently incomplete. Often patients leave them in their cars or lying around their offices waiting for the next doctor's appointment. As patients go from appointment to appointment, various providers may be viewing the medical information for the first time. Often they are unfamiliar with the patient's personal circumstances or individual condition; this is particularly challenging when a provider needs to make an urgent decision. While precious time passes, the provider begins the cumbersome (and perhaps desperate) process of assembling records to evaluate the patient's condition. Enter the concept of health information exchange, which can be a serious game-changer for patients.

Health information exchange (HIE) refers to the transfer of health information electronically, in accordance with national standards that ensure confidentiality, privacy and security.[1] A health information organization (HIO), by contrast, is the overseer. It is the mechanism that governs the exchange of the information between and among doctors, nurses, pharmacists and healthcare providers, in accordance with national standards.[2] (Quite simply, the HIE is a verb and the HIO is a noun; the HIO is the entity that facilitates the exchange of the information.) Along similar lines, interoperability is the capacity of information systems and applications to communicate with one another, and to exchange and use data through an automated approach.[3] It enables systems to work together to advance the delivery of healthcare.

The widespread exchange of health information raises obvious questions surrounding patient privacy and security. How is the HIO classified, and how do patients ensure their information will be safe and secure? Who is responsible for protecting the patient's protected health information? Do patients want providers to use HIE, and should there be limitations for specific types of information? And if so, what types of information?

On balance, the ability of patients to effectively manage their health through HIE seems to outweigh the confidentiality issues, provided appropriate safeguards are in place. In order to further the development of HIE and promote effective nationwide interoperability, the stakeholders involved must employ a shared agenda to educate the patient about this important process.

What Do Patients Want?

More than ever, patients require immediate answers—but not at the expense of their privacy. Perhaps they have been recently diagnosed with an illness and are wading through a maze of specialists to obtain a prognosis and develop a plan of care. Alternatively, they may have an accident or suffer an illness while traveling, causing an out-of-state provider to review their medical histories in order to make a complete assessment. Regardless of the circumstances, one thing is certain: Patients have no patience for sitting in a doctor's office waiting for multiple providers to interact with one another. Without seamless access to information, providers are forced to make split decisions using their best—but not always their most informed—medical judgment. Patients recognize these challenges facing providers, and the obvious need for various parties to communicate seamlessly in order to promote rapid and effective care.

As the sophistication level of HIOs and the publicity surrounding them has increased, patients have recognized the benefits of participating in these models.[4] Nevertheless, concerns still exist over confidentiality and potential security breaches.[5] These concerns especially ring true in the face of numerous significant data breaches that have plagued the healthcare industry. In fact, the year 2015 has been referred to as the "year of the health-care data breach," with healthcare having surpassed the financial and retail sectors as the most targeted industry for this egregious activity.[6] Information available as of this writing indicates that in 2015, the Office for Civil Rights (OCR) received notice of 254 healthcare data breaches, which collectively exposed the protected health information of more than 113 million individuals.[7] Even a cursory review of the OCR's breach report results for breaches affecting 500 or more individuals (a/k/a the infamous 'Wall of Shame') confirms that the vast majority of incidents arose from theft, which points to an absence of effective security measures.[8]

HIO Classification under HIPAA

A crucial starting point in evaluating the privacy obligations applicable to the HIO is a review of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, HIPAA).[9] The HIO is not a health plan, healthcare clearinghouse or healthcare provider who transmits health information in electronic form in connection with a transaction covered by the HIPAA rules. Thus, it is not a covered entity.[10] The HIO instead functions as a business associate, handling protected health information on behalf of various different covered entities.[11] In that capacity, it maintains access to protected health information on a regular basis for the limited purpose of sharing that information between myriad providers.[12]

The federal regulations require the HIO to enter into a written business associate agreement (BAA) in order to create, receive, maintain or transmit electronic protected health information. Thus, in order for it to exchange data between and among the providers, the HIO must have a BAA with them.[13] Under the privacy rule, covered entities that participate in an HIO are permitted to execute a single BAA that can be signed by the HIO (as the business associate) and by each of the covered entities; multiple BAAs between the HIO and each covered entity are not required.[14] Through these BAAs, the HIO agrees to maintain certain physical, administrative and technical safeguards, as prescribed by the HIPAA security rule.

The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, required business associates for the first time to comply with the HIPAA security rule, and authorized the imposition of civil monetary penalties against business associates for impermissible uses and disclosures of protected health information.[15] These stringent obligations have forced business associates to enhance risk analyses—developing policies and procedures, administering training programs, and accepting responsibility for protected health information. They must report security incidents and make breach notification to the covered entities in a timely manner.

Patient Awareness and Consent

Educating patients on the benefits of HIE and allowing them to have an active role in their healthcare (including obtaining consent to share data even when it is not legally required) will help to further confidence in HIE.

In general, HIPAA permits covered entities to freely transfer protected health information without patient authorization for purposes of treatment, payment and healthcare operations (*i.e.*, quality assessment/improvement and care management) purposes.[16] Nonetheless, exceptions to the "treatment, payment and health care operations" rule exist for certain categories of sensitive information, including substance abuse, HIV, mental health and abortion. Federal regulations that apply to alcohol and drug abuse patient records maintained in connection with federally assisted alcohol and drug abuse treatment facilities and programs administered by the Substance Abuse and Mental Health Services Administration (SAMHSA) require patients to consent to the disclosure of all records for treatment purposes, absent limited exceptions (*i.e.*, emergencies).[17] Likewise, various other federal and state laws require specific consent prior to the dissemination of information in sensitive categories prior to disclosure for treatment purposes.

HIPAA is a floor; as such, states can, and do, adopt more stringent standards in certain cases.[18]

This lack of consistency involving certain types of records presents an obvious problem in the context of HIE. What happens if the HIO needs to transmit information to or from a state that has specific consent requirements? What about an HIO that wants to transmit sensitive data (as opposed to simple 'treatment, payment, healthcare operations' data)?

One possibility for addressing this lack of consistency is for providers to obtain consent for any disclosure through the HIO, including disclosures for routine treatment, payment and healthcare operations purposes.[19] While this may seem like overkill, it would avoid the need for the segmentation of data (described below) and for evaluating every individual situation. Alternatively, providers could design a process that enables a patient to restrict certain types of information or certain types of recipients of their information.[20] Although the privacy rule does not require patient consent to participate in HIE, informing patients of these models and providing them with freedom of choice necessarily enhances their trust in the system.[21]

Providers can also make patients aware of their participation in HIE through distribution of notice of privacy practices (NPP). Under the HIPAA privacy rule, providers are required to furnish an NPP to patients on the date they receive their first service; the NPP identifies in plain language the ways the covered entity may use and disclose their protected health information.[22] While the HIO (as a non-provider) has no obligation to distribute the NPP, the providers participating in the HIO can disclose information relating to the HIO and identify the safeguards in place to protect the networked data.[23] Such an open and transparent process can also help facilitate patient trust in HIE.

Along the same lines, providers can consider distributing a standalone notice of disclosures relating to the HIO, specifically highlighting the issue and describing the protections in place (in the hopes that distinguishing these disclosures from the NPP will call attention to them). These options for sharing information with patients may stimulate trust and encourage the selection of providers that offer these cutting-edge options.

Quite simply, why wouldn't a patient want to participate in a system that facilitates seamless care, provided safeguards are in place and there is minimal risk in doing so?

The Advancement of HIE/HIO

The appropriate governmental agencies have continued to support the development of technological solutions that advance the progress of HIE. The HITECH Act initially established the Health Information Technology Policy Committee, which was charged with the responsibility for making recommendations to the Office of National Coordinator for Health IT (ONC) regarding HIE.[24]

The ONC has recognized that many patients will avoid seeking treatment if they do not believe their providers will be able to properly safeguard sensitive information contained in their medical records. With this in mind, the committee was principally charged with developing technologies that facilitate the segmentation of sensitive data through secure methods.[25] By employing data segmentation, the HIO can sequester (or set aside) such data and, through proper technology, the system can be coded to trigger the need for patient consent before the release of the sensitive information.

Various offices in the ONC also conducted and funded the data segmentation for privacy (DS4P) initiative, engaging a team of experts in health information technology to assess the handling of sensitive data relative to HIE.[26] The first phase of that initiative took place between 2011 and 2014. At its conclusion, the initiative produced a number of test cases that showed promising ability to exchange sensitive health information in a safe and secure manner.

The ONC will continue its focus on supporting the development of technology in this important area, educating providers on data segmentation and helping to ensure they can accept segmented data.[27] Reports suggest that additional pilot cases to evaluate the progress of HIE will be forthcoming.[28] In addition, the ONC has issued a comprehensive report expanding upon its initial set of guiding principles and building blocks for furthering HIE.[29] That report includes a set of 10 core items and an extensive plan that is specifically designed to advance HIE development, with the goal of achieving nationwide interoperability by the year 2024.

Conclusion

Clearly there is the crucial need for healthcare providers to coordinate care in order to reduce duplication of efforts, facilitate rapid decision-making and deliver better outcomes. HIE is a powerful tool to aid in this effort. Nonetheless, confidentiality concerns still exist.

Patients want better care, and support the sharing of information to get it only if they can be assured there will be no risk to their privacy. This is especially true when dealing with protected health information that would cause a stigma for a patient if it were to be released improperly.

At the root of it all, the author believes the federal government, state, tribal and local governments and the private sector need to develop a shared agenda in order for HIE to flourish and succeed.[30] It is essential for governmental agencies to continue to support the development of a strong and flexible health IT ecosystem that promotes the continuity of care through HIE and increases transparency.[31] The author believes development of safe and secure technical systems, coupled with patient education and enabling patients to take a meaningful role in their healthcare, is the only way to achieve the ONC's goal of nationwide interoperability according to plan.

***Deborah A. Cmielewski** is a partner with Schenck, Price, Smith & King, LLP, based in the Florham Park office. She is a member of the healthcare law and corporate practice groups and serves as the co-chair of the firm's pharmaceutical industry and pharmacy practice group.*

ENDNOTES

[1] The National Alliance for Health Information Technology Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms, 22-23 (April 28, 2008).

[2] *Id.* at 24. Notably, in the 2013 Omnibus Rulemaking, the United States Department of Health and Human Services specifically declined to modify the federal regulations to include a definition for HIO, noting instead that the industry continues to evolve and it will be more appropriate to issue guidance that can be periodically updated. 78 Fed. Reg. 5571 (Jan. 25, 2013).

[3] HIMSS definition of interoperability, approved by the HIMSS Board of Directors (April 5, 2013), available at himss.org/library/interoperability-standards/what - is - interoperability; *see also* the Office of the National Coordinator for Health Information Technology, Connecting Health and Care for the Nation: A Shared Nationwide Interoperability Roadmap, FINAL Version 1.0, x.

[4] Akanksha Jayanthi, Patients want interoperability, and here's how they want it: 6 key findings, Sept. 28, 2015.

[5] *Id.*

[6] 2015: The Year of the Healthcare Data Breach, *HIPAA Journal*, Dec. 29, 2015.

[7] *Id.*

[8] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[9] Pub. L. No. 104-191, 110 Stat. 1936 (Aug. 21, 1996).

[10] 45 C.F.R. § 160.103; Office of Civil Rights (OCR), The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment, Introduction, 3.

[11] The 2013 Omnibus Rulemaking added a number of new categories of business associates, including specifically the HIO. *See* Omnibus, *supra* note 2. *See also* 45 C.F.R. § 160.103.

[12] *Id.*

[13] 45 C.F.R. § 164.504.

[14] OCR, Introduction, *supra* note 10. *See also* OCR, The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment, Accountability, 5.

[15] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (Feb. 17, 2009).

[16] 45 C.F.R. §§ 164.501, 506.

[17] 42 C.F.R. Part 2. Particularly in the area of sensitive information, many providers have found it easier to simply avoid participation in HIE due to the challenges associated with obtaining and documenting the proper consents. SAMHSA Behavioral Health IT Webinar Series—Opioid Treatment Programs Service Continuity Pilot (Sept. 22, 2015).

[18] 45 C.F.R. §§ 160.202, 203.

[19] OCR, The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment, Individual Choice, 2.

[20] *Id.* at 5.

[21] Patient Consent for eHIT, Health Information Privacy Law and Policy, available at healthit.gov/providers-professionals/patient-consent-electronic-health-information.

[22] 45 C.F.R. § 164.520.

[23] OCR, The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment, Openness and Transparency, 2.

[24] 42 U.S.C. § 300jj.

[25] *Id.*

[26] HealthIT.gov, Enabling Privacy: Data Segmentation Overview, available at health.it.gov/providers-professionals/data-segmentation-overview.

[27] *Id.*

[28] Letter from Paul Tang, Vice Chair, HIT Policy Committee to Karen DeSalvo, M.D., National Coordinator for Health Information Technology, July 15, 2014. *See also* SAMHSA webinar, *supra* note 17; SAMHSA webinar, Integrating Behavioral Health into Health Information Exchanges (HIE) (Dec. 16, 2015).

[29] *See* National Alliance Report, *supra* note 1.

[30] *Id.*

[31] *Id.*

This article was originally published in the April 2016 issue of New Jersey Lawyer, a publication of the New Jersey State Bar Association, and is reprinted here with permission.