Possible Solutions to the Harmonization of Federal and State Privacy Laws for Health Information Exchanges

Katie Potorac
Institute for e-Health Policy
May 19, 2014

“The opinions in this paper are those of the author and not HIMSS or the Institute for e-Health Policy/HIMSS Foundation.”
Possible Solutions to the Harmonization of Federal and State Privacy Laws for Health Information Exchanges

Introduction

According to the Office of the National Coordinator for Health IT (ONC), “over several decades, states have passed laws to protect the privacy of health information. These laws frequently differ from state to state and often narrowly target a particular population, health condition, data collection effort, or specific types of health care organizations. As a result of these laws, the United States has a patchwork of privacy protections that are not comprehensive or easily understood” (1). According to the 2012 Report on Health Information Exchange, stakeholders believe that privacy and confidentiality are a moderate or substantial challenge and voted that it was the second highest issue concerning data exchange (2). Since the passing of The Health Insurance Portability and Accountability Act in 1996, states have had a more concrete standard to launch off into healthcare privacy laws. Health Information exchanges are increasing and their impact for healthcare is increasing as well. Knowing that the information flow of patients’ health information is growing, it is imperative to continue to improve legislation and regulations concerning privacy and security.

This problem is especially potent in areas where states are closely bordering each other. New York, New Jersey, and Connecticut form a tri-state area which geographically forces providers to work together, yet these providers are hindered by conflicting state privacy laws. Virginia, Maryland, and the District of Columbia also are part of a tri-state area which closely works together. Many physicians may even live in one of the states and commute to another for work. They may know another skilled provider from their state, yet have problems sharing health information because of state privacy laws. If these conflicting state issues were resolved, health information exchanges would have the opportunity to drastically increase its sphere of influence and the quality of care for patients would significantly increase.

Background

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law in 1996 and establishes national standards for protecting patient’s Protected Health Information. The law required the US Department of Health and Human Services to institute regulations for privacy and security, now known as HIPAA Privacy and HIPAA Security Rules.

HIPAA Privacy Rule institutes “national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safety measures to protect the privacy of protected health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patients’ rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections” (7).
HIPAA Security Rule formed “national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and availability of electronic protected health information” (8).

State laws that are contrary to the federal law will be preempted by HIPAA. The term “contrary” is defined as providers not being able to comply with both state and federal law or that the requirements of the state law prevent providers from observing the goals of HIPAA regulations. If however, a state has privacy laws that are “contrary” with HIPAA Privacy Rule, but are more stringent than HIPAA guidelines, the state laws will apply. The three exceptions to HIPAA Privacy Rule preemption are when the state law: “(1) relates to the privacy of individually identifiable health information and provides greater privacy protections or privacy rights with respect to such information (“more stringent”); (2) provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) requires certain health plan reporting, such as for management or financial audits” (9). State laws that are not contrary to HIPAA, but are more rigid should be followed.

New York, New Jersey, and Connecticut Privacy State Laws

New York

Out of the entire United States, New York is rated as one of the highest state for Health Information Exchanges (HIEs), second only to California, and it had the most advanced Health Information initiatives in 2012 (2). Because New York is so far ahead of the times in comparison to other states, much of their legislation is also more stringent than HIPAA and therefore is not preempted. Public Health Law (PHL) Section 17 from 2002 states "Upon the written request. . . [of a patient, a provider] . . . must release and deliver . . . copies of all . . . medical records . . . regarding that patient to any other designated physician or hospital. . .". However, the HIPAA Privacy Rule states “a ‘covered entity’ may generally disclose ‘protected health information’ (PHI) to another covered entity for treatment, payment or health care operations without consent (164.506(a), 164.506(c)). A covered entity may use or disclose PHI without an authorization or opportunity to agree or object to the extent that such use or disclosure is "required by law". Because PHL Section 17 requires that providers seek patient authorization before disclosure of health records and is therefore more rigorous than HIPAA, PHL 17 will take precedence. PHL Section 17 also conditions that providers do not disclose information of venereal disease or abortions of un-emancipated minors to their parents or legal guardians. This law is also more inflexible then HIPAA so it takes precedence.

PHL Section 18 applies to any health care provider as predetermined in New York state law and it also applies to information concerning the examination, health assessment, or treatment of an individual. HIPAA applies to any “covered entity”: health care provider, health care clearinghouse, or health plan. It also relates to all medical records and billing records and any other records used to made decisions about individuals. Because HIPAA is more rigid in both cases of PHL Section 18, HIPAA takes precedence. There are however exceptions to the general rule and in some circumstances, PHL Section 18 is found to stand over HIPAA (11). In most cases, New York law is found to be stronger than HIPAA and allowed to take precedence.

New Jersey
The New Jersey state privacy laws are less detailed compared to New York and HIPAA because there are no forms provided and it contains less instruction as to content, process or method (14). The New Jersey law has been found to be about as stringent as HIPAA. “NJ Admin Code Section 8.43G-4.1 states: Every hospital patient has a right to "promptly access" information in his or her medical record, and has the right to obtain a copy of such record within 30 days of a written request. NJ Admin Code Section 13:35-6.5: A health care practitioner must provide a copy or a summary of a patient’s treatment or billing records within 30 days of receiving a request” (13). Overall, New Jersey law is the same as HIPAA and therefore can be followed without contradiction to HIPAA.

Also, New Jersey has been leading efforts for multi-state collaboration for Health Information Exchanges. All initiatives will be according to Healtheway standards. These initiatives include hosting a multi-state collaboration event with surrounding states to focus on sharing of plans and establishing an approach for secure HIE. Also, New Jersey wants to launch a project management focus on multi-state pilots by overseeing and coordinate several interstate secure HIE pilot initiatives. Lastly, NJ wishes to implement a regional health information exchange organization (RHIO) with Fox Chase Cancer Center HIE’s in Philadelphia, Pennsylvania (15).

Connecticut

Connecticut privacy laws very similarly follows HIPAA privacy rule so it takes precedence. Connecticut law states, “Connecticut General Statuses Annotated (CGSA) Section 20-7c: Health care providers must furnish a copy of the medical record within 30 days from a patient’s request” (13). Also, Section 20-7d states that “a copy of the patient’s health record, including but not limited to, x-rays and copies of laboratory reports, prescriptions and other technical information used in assessing the patient’s condition shall be furnished to another provider upon the request of the patient”. Because Connecticut law is found to be more rigid than HIPAA, Section 20-7d takes precedence.

Overview

New Jersey and Connecticut are found to contain privacy laws that comply with HIPAA regulations and are not contradictory. In this case, HIPAA does not preempt New Jersey and Connecticut law. New York, however, is more stringent and therefore New York privacy law takes precedence. With differing privacy laws, it would be very difficult for New York and Connecticut or New York and New Jersey to communicate for health information exchange. A primary care physician (PCP) in New Jersey may not know of any experienced specialists in the state, but he may know of a specialist in New York, within 10 miles from his practice. Yet because of the need to follow different privacy laws across state borders, this PCP may not have the ability to have open and honest communication about the care of his patient. Even with the similarities in legislation between New Jersey and Connecticut, either state may have a specific clause for the care of a certain type of patient. Mental health, drug abuse, minors, and other categories have distinctive laws in place pertaining to their record keeping and sharing of medical information. These boundaries make it difficult for physicians to seek help from providers in other states.

Virginia, Maryland, District of Columbia Privacy State Laws
Virginia privacy law is more rigid than HIPAA in many aspects and will take precedence. The Annotated Code of VA Section 32.1-127.1:03 state that “Health care entities must disclose a patient's health care records to a patient in accordance with a written request for disclosure. Health care entities must furnish copies of or allow access to a patient's health care records in an electronic format within 15 days of receiving a written request for access to such records. VA Code Ann. Section 54.1-2403.3: Health care practitioners must release copies of a patient's medical records in compliance with requirements applicable to health care entities (see also 18 VA Admin Code Section 85-20-26). The laws do not specify a time period for access to records in a hard copy (e.g., paper) format”.

Maryland privacy law is stronger than HIPAA and therefore takes precedence. There are still certain exceptions, but Maryland law states that “MD Code, Health-General Section 4-309: A health care provider or hospital must provide a patient access to his or her medical records within 21 days from the request” (15). HIPAA law just stipulates a reasonable time and Maryland restricts providers to 21 days after receiving a request for medical records.

District of Columbia

DC Privacy law is considered to be consistent with HIPAA law and therefore takes precedence. DC ST Section 3-1210.11 states that, “Health care providers must provide a patient with his or her medical record within a "reasonable time" from the request, which has been further defined by 17 DCMR Section 4612 to mean within 30 days of the request”. Because DC law follows HIPAA law with having a reasonable time for providers to respond to patients and then specifying 30 days as a reasonable time, DC law continues to take precedence.

Overview

Since Virginia and Maryland have more rigid laws than HIPAA, their state privacy laws take precedence. DC privacy law also takes precedence, but only because it is consistent with HIPAA privacy regulations. Again, physicians are hard pressed to provide the best quality care and to follow varying state and federal privacy regulations. Even if a PCP has a good professional experience with a cardiologist in a bordering state, they may not continue their relationship because the PCP does not want to deal with legal ramifications. It might be easier to send the patient to a cardiologist who the PCP knows is not as good as the other one. This hampering of medical care could lead to detrimental effects for the provider, and most importantly, the patient. If states work together to enable health information exchange, more promising solutions will be available.

Solutions

Health Information Organizations

Health Information exchanges are rising and under the “State Health Information Exchange Cooperative Agreement Program (SHIECAP), 56 states, eligible territories, or qualified State Designated Entities (SDEs) in the US received funding from the ONC to support HIE within and across states” (2). The purpose is to ease and
enlarge the scope of secure electronic transport of health information across the country based on nationwide standards. Health Information Exchanges are meant to improve patient quality of care, safety, productivity, research advancements, and will eventually enhance health care for the general public of the United States.

These types of nationwide health exchanges are happening with different providers and organizations across the United States. The newly announced Mid-States Consortium of Health Information Organizations will include sixteen regional and statewide health information exchanges to build trust and remove barriers to share patient data. Laura McCrany, executive director of Kansas Health Information Network shares that, “The goal is to ensure important patient information is available at the point of care. We recognize our patients cross state lines and our health information organizations are regional or state based and we have to connect those organizations together” (18). The organizations state that choosing the technology to be used is the easy part, while agreeing on the governance of privacy and security will come later this year.

**Contractual Agreements**

Prior to 2009, business entities were not subject to HIPAA directly and therefore formed their own Contractual Agreements, which are specific contracts in place before allowing business associates access to protected health information (PHI). Under HIPAA’s indirect terms, business associates needed to ensure that they would effectively secure and not mishandle PHI (19).

As a result of the passage of the HITECH Act in 2009, the government has enlarged jurisdiction over the confidentiality and protection of PHI to business associates and the business associates are obligated to abide by the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule. If a subcontractor provides data communication services that do not necessitate access to PHI except on an irregular and occasional basis, then they would not be considered business associates (19).

Finally, it is vital for the federal government to understand that passage of the HITECH Act has greatly impacted business associates, as well as countless providers and patients involved. The Omnibus Rule heightened civil monetary penalties and now covered entities and business associates are paying attention to HIPAA compliance, now more than ever.

**Conclusion**

HIMSS recommends that Congress continue to support harmonization of federal and state privacy laws by being aware of the barriers to information exchange created by the contrasting laws and regulations, supporting interoperability standards for Health Information Organizations, continuing funding new efforts for health information exchange (20).
References