# The Travel of Privacy Standards and Regulations in Healthcare

Chad Anderson
Miami University
ander556@miamioh.edu

Richard Baskerville
Georgia State University
Curtin University
baskerville@acm.org

Mala Kaul
University of Nevada, Reno
mkaul@unr.edu

## Abstract

*Increasing technology dependence by individuals and organizations has resulted in a profusion of information privacy standards and regulations created to protect personal information. There are expectations of universality in the scope of standards and regulations but also, in most cases, some degree of flexibility that allows for adaptation and compliance with local requirements and influences. Our research into the privacy policy development at a health information exchange (HIE) finds that in practice, standards and regulations are subject to multiple translations that can result in policies and practices which inhibit the HIE's goal of facilitating data exchange. Translation must therefore be appropriately managed by the HIE to ensure data exchange is not constrained. This has important theoretical and practical implications for health information privacy in an increasingly technology pervasive world, by contrasting the global view with the local view of information privacy, through an application of healthcare standards setting and execution.*

## 1. Introduction

With increasing digitalization of information there is a growing concern for how the privacy of information can be maintained [16] and new research to understand the factors affecting its security [2, 17]. Standards and regulations are mechanisms to homogenize information privacy and security practices with the expectation that this will improve the privacy and security of protected information. It has long been known that the practices of privacy and security standards-setting emerge from a highly socialized context of power, politics, and organizational players [4]. Nevertheless, much of the work done in the development of privacy laws and guidelines assumes that such formulations set universal standards for the protection of sensitive, personally identifiable information [15, 18]. However, despite international agreements on privacy rights [27], it is widely recognized that the implementation and regulation of privacy varies significantly across nations [11], regions [19], organizations [14], and even types of data [33].

That variability can be a significant problem for organizations that seek to create platforms through which other organizations can connect and share data. A health information exchange (HIE) is one such organization and many HIEs in the United States have struggled to achieve their purpose of facilitating interoperability and health data exchange [37]. That challenge has particularly been evidenced in the years following the 2009 HITECH Act, which funded HIE development in every state and U.S. territory [9].

Our goal in this paper is to demonstrate, with the use of *translation theory* [6], how meaningful variations in organizational privacy policies and practices occur in spite of standards and regulations to create consistency across organizations and how those variations can be managed to keep them from seriously impacting the participation in and value of interorganizational information exchange.

## 2. Theoretical Background

We focus on information privacy, but also address information security, as the two concepts are interrelated. The relationship lies in the need for effective information security to protect privacy. Security encompasses the protection of information confidentiality, integrity, and availability. However, properly secured information might still be subject to privacy abuses if the organization makes bad decisions about information uses. Privacy policies define how an organization uses certain types of information and therefore, effective security policies are necessary for privacy, but insufficient without effective privacy policies [1, 34]. In this paper we draw on several research areas such as setting of standards in general, setting of privacy and security standards in particular, and the theoretical background for how ideas travel from one setting to another. The concept of the travel of ideas will be used to demonstrate the adaptation of privacy standards in local or discrete settings.

### 2.1 Standards

URI: https://hdl.handle.net/10125/71083
978-0-9981331-4-0

The standardization movement emerged as a component of two forces: the industrial revolution with mass production prioritizing cheap, standardized products over more expensive individualized ones [20], and the progress of globalization needed to extend markets and manufacturing across borders. The setting of standards is tightly related to regulatory administration, while being adverse to political influence on the content of the standards [39]. Nevertheless, there can be enormous pressure on the standards-setting process from various stakeholders, such as organizations and institutions with vested interests in the competing range of possible standards. This pressure can affect the level of due process that is followed by standards-setting bodies [10]. Further, technological developments impact standards setting as technology, institutions, and industry structure can be organized in different ways, such as a more open structure or a more vertically integrated structure. In other words, not only do technology and standards co-evolve, technology and the process of standards-setting co-evolve [10].

### 2.2 Information Security Standards and Regulations

The emergence of information security standards and regulations, including privacy, is a result of the standards movement, but the increasing development and use of security standards is also connected with difficulties in using traditional risk analysis calculations for developing economic justification for the acquisition of security controls [13]. A risk analysis approach often involves complex calculations on questionable data, which fails to economically justify some of the most basic and essential security safeguards. Consequently, if organizations follow a security standard, justification for the acquisition of proper safeguards according to that standard can carry more weight with management than using economic risk analysis. This shifting practice is further influenced by increasing legal requirements for auditors to review information security who tend to use widely recognized standards as their basis for auditing systems. This provides an additional rationale for using standards as the basis for selecting and implementing controls in the first place.

With regard to individual data privacy, there are a few additional reasons that support standard setting. One reason is to avoid any misunderstanding between various national data protection authorities [30]. Another reason is to prevent the disparities in national legislations from hindering transnational free-flow of personal data [28, 33]. Of course, the development and enforcement of standards must also be weighed against the cost of those standards to organizations and individual consumers [35]. Standards and regulations operate on varying levels of scope, which result in layers of standards and regulations. Some standards are international in scope (e.g., General Data Protection Regulation) while others are promulgated by national governments as laws (e.g., U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996). Still others are developed by professional organizations as standards of professional practice (e.g., Control Objectives for Information and Related Technology (COBIT) Framework) or by industry groups as requirements within a given industry (e.g., Payment Card Industry (PCI) Security Standards).

### 2.3 Translation Theory

The diffusion perspective holds that ideas apply across settings in a way that is more-or-less intact and the effects of different contexts will not meaningfully change the ideas themselves [5]. Czarniawska & Joerges [6] challenge this notion by theorizing that ideas travel from place-to-place and from time-to-time and, like any traveler, they are changed by the travel experience. In other words, importing an idea from one setting to another is a movement across time and space with movement through either dimension engendering change.

Translation theory was originally developed by Michel Serres and then adapted to sociology by Michel Callon who incorporated it into Actor Network Theory [21]. A key characteristic of translation theory is that universal or global ideas have no independent existence. Rather, translation theory regards global ideas (such as a privacy standard) as simply a network of interconnected local ideas. This network embodies translocal ideas (i.e., a network of local ideas that inhabit various localities) rather than global ideas [6]. In other words, translation theory does not distinguish between local and global ideas; rather it distinguishes between local and translocal ideas [5].

For Czarniawska and Joerges [6], ideas travel through their movement across time and space from one local setting to another. This travel is similar to Giddens' [12] description of how concepts could be disembedded from one context and re-embedded in another. Before any idea can travel into a new local setting, it must first be translated from its form as found in its previous local setting. Callon and Latour state that "By translation, we understand all the negotiations, intrigues, calculations, acts of persuasion and violence, thanks to which an actor or force takes or causes to be conferred on itself, authority to speak or act on behalf of another actor or force." [21, p. 279]

Translation of an idea spans from one local place to another local place. It uses and creates ambiguity in order to make subtle changes to the meaning of structures or the conduct of practical actions. The origin

of such translation is found in the "inequivalence" between meanings (and interests) in two different localities. The process of translation resolves this inequivalence through mediation, invention, displacement and revised linkages between concepts [6, p. 24]. Therefore, as privacy standards and regulations travel, the translation of their structures and practical actions will modify them. Further, this translation can also change the individuals who are following these standards and regulations. For example, as privacy standards and regulations travel to a new locality, their translation may modify their structures to subtly shift power relationships (e.g., a privacy officer in one locality may have a different role than a privacy officer in another locality). In other words, translation can change individuals' social positions.

Prior research in information systems has used translation theory to understand the impact of existing power networks, organizational culture and subcultures in IT management [8], how Internet and e-commerce travel to older people [36], the travel of knowledge in project management [3], the travel of relational practices between middle managers in Sweden and China [7], the process of IT institutionalization through the travel of ideas about IT usage in home care [26] and the study of differences in agile method adoption between different organizations [29].

## 3. Research Design

The HITECH Act of 2009 provided nearly $550 million in federal funding for the development of HIEs in every state and U.S. territory. The limited success of those initiatives [9] led us to investigate what factors contribute to an HIE's success. Security and privacy are important elements of any information exchange process and since policies provide the framework through which information security and privacy behaviors and outcomes occur, we focused our inquiry into the development and implementation of an HIE's information security and privacy policies. We employed a qualitative case study design, which enables a detailed exploration of complex phenomena in real-world settings [38].

### 3.1 Data Collection

The successful HIE that we studied was created in 2011 to support health information exchange needs in a western U.S. state and will henceforth be called HealthEx. This was a longitudinal study to uncover how HealthEx's information security and privacy policies were developed and implemented over time, and how those processes contributed to the success of the HIE. We used a qualitative research approach for the flexibility needed to pursue emergent avenues of inquiry [23]. The discovery of layers of translation present in the implementation of HealthEx's privacy policies was one such emergent avenue.

HealthEx's executive director coordinated access for data collection by arranging meetings and providing contact information for available participants in HealthEx's information security policy development process. We conducted semi-structured interviews with these participants, either in person or by telephone. All interviews, but one, were recorded for later analysis. Where led by our line of inquiry, we pursued emerging ideas both within specific interviews and by arranging subsequent interviews [23]. We also collected and analyzed documentation, including the different versions of the security and privacy policies, policy development timelines, and the document deliverables at each stage of the policy development process.

HealthEx was created by the state's Quality Improvement Organization (QIO) at the behest of individuals in the state's healthcare community. To set up the HIE, the QIO hired a consultant who was an expert on HIE development and federal laws pertaining to health information exchange. The QIO also invited members of the state's healthcare community to participate in the HIE development process both to draw on their expertise (e.g., knowledge of state law and current practices within the state) and to generate buy-in as potential participants in the exchange.

Eight task forces were set up to develop component plans for the HIE with each comprised of HIE staff and members of the state's healthcare community who were subject matter experts on healthcare operations, health information management, and legal issues in the healthcare environment. The privacy and security task force developed a roadmap for the HIE's privacy and security policies by looking at federal and state regulations. The focus, with regard to federal regulation, was HIPAA as noted by the External Consultant who said *"We always start with the [HIPAA] standards, that's where we go first and how do you meet each one of them."* State statutes were also considered as noted by the HIT Director who stated *"A lot of time was spent reviewing state statute and how we would ensure that we're compliant with that state statute."* The resulting roadmap was then used to write the actual policies.

Our first round of data collection took place in the first half of 2015 and included interviews with six members of the HealthEx staff and the external consultant who was responsible for the initial creation of the HIE. At the end of 2016 we conducted a second round of data collection that included interviews with five members of the HealthEx staff. The interview

guides for both stages can be provided on request. This second round of interviews provided an opportunity to gather information on changes to the HIE's information security and privacy policies during the one-and-a-half-year period following the first round of interviews. There had also been significant turnover in the HealthEx staff as only two of the second-round interviewees (the executive director and a project coordinator who had been an intern) had been with the organization to participate in the first round of interviews. This provided us with the opportunity to assess the effects of new personnel on the evolution of the organization's information security and privacy policies. Table 1 shows the roles of all participants in each stage of data collection.

**Table 1. Study Participant Roles**

| Round 1 Participants | Round 2 Participants |
|---|---|
| Executive Director | Executive Director |
| HIT Director | HIE Director |
| Outreach Director | Assistant HIE Director |
| QIO Information | New QIO Information |
| Security Officer | Security Officer |
| Support Specialist | Project Coordinator |
| HIT Intern | |
| External Consultant | |

At the end of our second round of data collection HealthEx had 135 participating healthcare organizations representing a large and diverse portion of the state's healthcare community.

### 3.2 Data Analysis

We began data analysis immediately after the first interview with the goal of identifying elements of the information security and privacy policy development process that explained how HealthEx had been successful in developing and growing the exchange. That early analysis enabled us to adapt our data collection efforts as we identified new avenues of inquiry. We analyzed our interview transcripts and document data in an iterative process of data reduction and conclusion drawing [24]. The discovery of the layers of translation affecting HealthEx's policies led us to analyze the data using the lens of translation theory. The following section explains the layers of translation we identified in our analysis.

## 4. The Travel of Privacy Ideas: From OECD to HealthEx

In this section, we will unfold the travel of privacy ideas from one locality to another, treating entities, like the OECD and HealthEx, as localities where the translation of ideas take place. In the interest of space, we will confine our analysis to the ideas around individual consent in relation to the use and sharing of personal private information.

### 4.1 The Ideas at OECD

OECD privacy guidelines, first established in 1980, will serve as the starting point for the travel of information privacy ideas for this case. Three principles in the OECD guidelines relate to individual consent; the Use Limitation Principle, the Purpose Specification Principle, and the Collection Limitation Principle.

The *Use Limitation Principle* states, "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: (a) with the consent of the data subject; or (b) by the authority of law" (OECD, 2013, p. 75).

The *Purpose Specification Principle* states, "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose" (OECD, 2013, p. 75).

The *Collection Limitation Principle*, states, "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject" (OECD, 2013, p. 75).

These principles are meant to be applied broadly to all types of personal data collected by any organization. However, we can narrow the focus to health information by using terminology specific to healthcare where the OECD privacy principles would dictate that a healthcare provider should (a) specify the purpose(s) for collecting a patient's data, (b) obtain patient's consent to collect that data in order to provide specific health services, and (c) obtain patient's consent if that data is to be shared with other entities or used for any other purpose.

### 4.2 First Translation: The Ideas in HIPAA

In the U.S., HIPAA was the first federal legislation to specifically address privacy of health information and these privacy ideas were translations of global standards established by the OECD and other entities. This represents a travel of privacy ideas from the OECD locality to the HIPAA locality. HIPAA was written into federal law in 1996 but was updated with the Standards for Privacy of Individually Identifiable Health

Information (Privacy Rule) finalized in 2002 (OCR, 2002). The 2002 Privacy Rule removed an earlier requirement that "a covered health care provider with a direct treatment relationship with an individual must have obtained the individual's prior written consent for use or disclosure of protected health information for treatment, payment, or health care operations" (p. 75). The reason for this change was that, "The consent requirement posed many difficulties for an individual's access to health care and was problematic for operations essential for the quality of the health care delivery system" (p. 75-76). The Rule states that, "In eliminating the consent requirement, the Department preserves the opportunity for a covered health care provider with a direct treatment relationship with an individual to engage in a meaningful communication about the provider's privacy practices and the individual's rights" (p. 76). In other words, while consent is not required for disclosure of protected health information (PHI), a provider should still inform the patient of his/her rights regarding PHI privacy. This change to federal regulation was noted by the HIE's external consultant:

> *Having every patient sign authorization forms, it's not required by HIPAA. It might be required by your state law or your own policies, but HIPAA does not require it … But a lot of barriers have been put up by people that are either misinformed or over-interpreting those requirements (External Consultant).*

This is an example of how changes to standards in one locality can negatively affect the translation of those standards in another locality as policy developers may be working from old information or misinterpreting changes made to the referencing standard.

***Translation in the HIPAA locality*:** Providers have rights to decide issues about the privacy of healthcare information. Purpose specification, and any requirement for consent, is operationally problematic, and creates an economic burden in healthcare settings. In lieu of consent, individuals should be informed of their privacy rights.

### 4.3 Second Translation: The Ideas in ONC

New opportunities of online information exchange highlight the potential benefits of sharing health data, such as improving patient care and improving public health management. At the same time, there is a growing recognition of the challenges in keeping that information private and secure. Within that context, Executive Order 13335 created the Office of the National Coordinator for Health Information Technology (ONC) in 2004. In this locality, the ONC was charged with developing "a strategic plan to guide the nationwide implementation of interoperable health information technology" (ONC, 2008, p. 3). As part of its mission, the ONC produced the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.

This framework was created because, "Clear, understandable, uniform principles are a first step in developing a consistent and coordinated approach to privacy and security and a key component to building the trust required to realize the potential benefits of electronic health information exchange" (p. 2). The framework included a principle of "individual choice" specifying that, "Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information" (p. 9).

This principle does not define *how* choice is to be implemented but emphasizes that *choice is important*. Since the ONC framework is not a law, like HIPAA, health care organizations are not required to follow its principles. Rather, ONC encourages states and healthcare organizations to translate the HIPAA Privacy Rule to retain consent in state regulations and organization privacy policies. Achieving universalism requires tracing the costs and benefits associated with translations to achieve a reasonable balance between meeting local needs and achieving universality [31]. In the context of HIPAA and ONC, this balance becomes more important when universality is achieved through enforceable laws vs voluntary frameworks. Specifically, in this case, HIPAA lawmakers saw that requiring consent to share patient information to achieve universality of strong patient privacy would create an imbalance between the cost of collecting consent and the benefit of sharing patient information. Forcing consent was expected to result in less information sharing between providers, which was opposite to the goal of increasing information sharing. Therefore, the legal requirement for consent under HIPAA was limited to patients being informed about their rights. In contrast, the voluntary nature of the ONC framework allowed for a stronger privacy recommendation for patients to have a choice regarding the collection and use of their PHI.

***Translation in the ONC locality*:** Privacy rights are an informed individual's choice. Inform individuals about their privacy rights and give them the choice in collecting, using, and sharing the data about them.

### 4.4 Third Translation: The Ideas in HealthEx's State

In the US, in addition to federal laws, states have enacted their own statutes and created health privacy

regulation that may be stricter than HIPAA. HealthEx's state developed a statute regarding health data sharing that included specific requirements for patient consent. In this locality, the state had enacted a law that states:

> *A covered entity that makes individually identifiable health information available electronically…shall allow any person to opt out of having his or her individually identifiable health information disclosed electronically to other covered entities, except…that a person who is a recipient of Medicaid or insurance pursuant to the Children's Health Insurance Program may not opt out" (NRS 439.538, 2013).*

This statute reflects a closer translation of the ONC framework than the HIPAA Privacy Rule with regard to patient consent.

***Translation in the state locality*:** Privacy rights are the right to opt out. Give individuals the opportunity to opt out of any sharing of data about them.

### 4.5 Fourth Translation: The Ideas in HealthEx

As described earlier, HealthEx had developed its policies based on HIPAA regulation and state statutes. In this locality, the Patient Consent policy reflects the state regulation on consent in its purpose statement:

> *To ensure confidentiality and privacy of electronic health records within the [HIE], patients must consent to having their records accessible through the HIE. Pursuant to NRS 439.538 a patient who is a recipient of Medicaid or insurance pursuant to the Children's Health Insurance Program will have his or her individual identifiable health information disclosed electronically (Policy # PVY.708.4).*

Here the organization's policy is a direct translation of the state regulation at the level of its purpose statement. To elaborate on how that purpose will be operationalized, the remainder of HealthEx's Patient Consent policy provides additional elaboration to describe the way in which consent must be obtained and documented. Specifically, HealthEx established an official consent form that all participant healthcare organizations had to use to collect patient consent. The consent form gives the patient three choices for sharing their PHI: I consent, I do not consent, or I consent only in case of an emergency. When a patient chooses "I consent" they are consenting to the sharing of all their PHI. They cannot designate some PHI to be shared, while other PHI is not shared.

This restriction is based on the capabilities of the HIE software which cannot limit sharing to specific types of information. The policy also requires officials at the participant organizations to witness the patient's signature and consent choice by signing and dating the form. Participant organizations are required to maintain copies of the signed forms for a minimum of six years. Patients may change their consent status at any time by completing a new form. In HealthEx's locality, the translation of ideas from other localities (e.g., HIPAA, state law) primarily reflects the need to follow the law and to operationalize those laws in the HIE.

***Translation in the HealthEx locality*:** Privacy rights are a Yes/No/Maybe decision.

### 4.6 Fifth Translation: The Ideas in HealthEx's Member Organizations

Operationalizing consent for the HIE was complicated by the fact that some member organizations had privacy policies that were much more restrictive than state and federal laws required.

> *The hospitals … may have developed policies that are more strict than HIPAA, … and sometimes going beyond even what the state laws require and that often can become a problem because the point of the HIE is to share the information, share the data in a secure way, but also you don't want to put up roadblocks to having providers and others being able to access information when they need it (External Consultant).*

This challenge was addressed by bringing together community members to create a policy that satisfied the needs of as many potential participants as possible without being overly restrictive.

> *"We met once a month for six months to bring the community back together and say, you're going to be the ones getting the consent. Where would this fit in doctor's office? How would you go about this? What would the flow be? And developing the policy for that, developing the form" (Executive Director).*

The community-based development of HIE's policies produced a translation of federal and state regulations that was likely different from what the HIE would have done on its own. Each time the HIE revised their policies, they sought feedback from participants about the impact of those changes on the participants. "We do send these policies out [to participants]. We look for feedback. Is there anything maybe we

overlooked that would be a concern to … participants?" (Support Specialist). This was particularly important for the consent policy as it was being operationalized by the participants. This ongoing interaction with participants to improve the HIE's policies further influenced translation of standards and the success of the HIE.

| ***Translations in the Member Organization localities*:** Privacy rights can be more or less precisely defined. |
|---|

Table 2 summarizes the translation of privacy rights into local ideas in various localities relating to HealthEx.

**Table 2. Travel of privacy ideas from one locality to another**

| Locality | Translation |
|---|---|
| HIPAA locality | Providers have rights to decide issues about the privacy of healthcare information |
| ONC locality | Privacy rights are an informed individual's choice |
| State locality | Privacy rights are the right to opt out |
| HealthEx locality | Privacy rights are a Yes/No/Maybe decision |
| Member Organization localities | Privacy rights can be more or less precisely defined |

## 5. Managing Translation

In the previous section we described and explained the translation of privacy standards and regulations for handling protected health information through various localities. We now turn our attention to the potential impacts of those translations and how HealthEx was able to manage them. While some translation is benign, for example, simply reflecting a more specific implementation of referencing ideas, other translation can be highly detrimental for certain localities. The primary danger in the context of an HIE is translation that goes too far in restricting data sharing. This is evidenced in the following two quotes illustrating overly restrictive interpretations of HIPAA and state statutes, respectively.

> *"Sometimes we have people say, well, we can't do this because of HIPAA and 90% of the time that's not a true statement. It's that they are misinterpreting HIPAA or over emphasizing the confidentiality aspect." (External Consultant)*

> *"There was one interpretation of the statute … that if you took the literal language and tried to apply it, you would have shut down electronic exchange of any health data in the state…Everything would have to have reverted to paper had you taken it with that interpretation and there were folks that looked at it that way." (HIE Director)*

We identified three areas where HealthEx had to address problems with translation: 1) internal privacy and security policy development, 2) development of state privacy regulation, and 3) existing privacy policies and practices in member organizations. We explain each of these by providing evidence for the problem and how HealthEx managed the translations to keep them from seriously harming the HIE.

First, HealthEx had to develop their own privacy and security policies to remain compliant with HIPAA and state statutes while also achieving their primary goal of enabling the exchange of health data between member organizations. They made the decision up front to gather input for an HIE roadmap from the state's healthcare community that started with a kickoff meeting. The Executive Director explained that *"we invited providers from all over the state. We paid for their way down. We bussed them to the venue."* In describing the makeup of the privacy and security task force, the External Consultant said *"We had several hospitals represented. We had HIM [health information management] professionals, at least a couple of privacy officers. So, I think we had very good representation from people that were very knowledgeable and very committed to the concept."* The HIT Director also noted that *"We brought together stakeholders not based on what an ONC or a CMS panel says should be on there. We brought stakeholders on based on the state's makeup."* In other words, HealthEx made a concerted initial effort to gather input from a knowledgeable and representative cross section of the community that would include potential participants in the HIE. There was an expectation that taking that approach was particularly important for privacy and security where translation was expected to be more of an issue as the HIT Director noted *"Our goal was not to set up the privacy and security in a silo, but to include all the players. One of the reasons we went down that path is a lot of privacy and security is about interpretation."* The result of those efforts was an effective road map for developing the internal privacy and security policies that guided HealthEx as they built out the HIE.

The second key requirement for HealthEx was compliance with state statutes. The HIE Director talked about how they initially struggled with that aspect of the policy development process. He stated, *"we had bad statutes and zero regulations on any statutes"*. This was

echoed by the Executive Director: *"we didn't have direction … from the state."* The lack of direction and good statutes created an environment where problems with translation of the statutes were inevitable. The Executive Director noted: *"You wouldn't believe the time and people on different sides of what the statute actually said."* Instead of waiting to see what would happen, HealthEx made the decision to get involved in the legislative process to shape the statutes. The HIT Director explained the reasoning for their decision as *"We need legislation that's not developed in a vacuum. We need legislation that's vetted by all the stakeholders…so we're working with the legislator."* The Executive Director participated in several legislative hearings on behalf of HealthEx to provide their voice on the statute development, *"I've testified twice including just last Friday…and I testified at the Health and Human Services hearing."* The result was a better-worded statute that clarified the consent process making organizations more willing to join the HIE.

The third area of concern for HealthEx was that member organizations would need to be compliant with their own policies in addition to the policies of the HIE. The HIT Director offered a scenario where *"If we go to large system A and say, no, we have to meet this over here, they're like, whoa, wait a minute, we have a business plan that we have to meet and you are an integral part of that, which means you have to comply with our privacy and security as well."* This was particularly important for HealthEx because 100% of their funding came from participant fees. The HIT Director noted that *"We had to meet market needs…to make sure that we have a product that's meeting our stakeholders needs that they're willing to pay for."* Involving member organizations in both the initial policy development process and later policy evaluation and update processes helped to ensure that conflicts between HealthEx's policies and member policies were effectively addressed.

## 6. Discussion

This research highlights the importance of the local context and how globally initiated privacy standards and regulations are translated across various localities. We found that global regulations undergo local translations in different settings and explain why it is important to recognize and manage these translations. Through this longitudinal case study, we have developed a number of insights into the travel of ideas about information privacy rights across various localities. The first is that core ideas can vary meaningfully from one locality to another. For example, in the OECD setting, the local ideas of the OECD privacy principles are influenced by the flow of individual data, (often economic), across international borders. Developing principles to be enacted into law by its member states enabled OECD to regard personal data in a broader context. It assigns higher rights to individuals over their information, than how others could treat this personal information. However, once these principles travel to the healthcare industry in the form of HIPAA legislation, certain parts of the OECD guidelines are discarded as unworkable and the organization must inform the individual. The localities and flows of translation are illustrated in Figure 1 below.

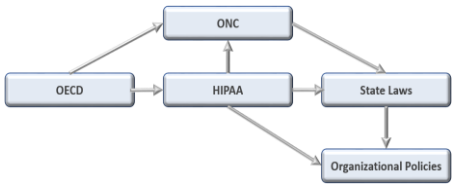


**Figure 1. Translation flows of standards and regulations across localities**

Under the influence of the evolving landscape of privacy law, the individual's privacy choice grows more prominent in some localities where, for example, individuals are entitled to opt out of the sharing of their health data beyond its original collection setting. Furthermore, a range of local policies will emerge among healthcare providers about how the opt-out regulation is implemented, and, in some cases, those local translations will conflict. Such conflicting translations are not necessarily "more right" or "more wrong" to the extent they are translations based on the cultures and values of individuals and organizations in the localities, but they can be detrimental to the goals of entities like HIEs when they inhibit participation in the exchange of data.

This paper makes a number of important contributions. We illustrate how localities are not necessarily geographic or even similar in nature or scope. For example, regulatory entities like the OECD and ONC are equivalent localities. States and business entities like HealthEx are equivalent localities. These are highly dissimilar localities, yet each is engaged in translating ideas from other localities for its own use. While OECD guidelines, HIPAA, and state laws could make claim to more-or-less limited universality, those limits underscore how the notion of global ideas is less useful than *trans-local ideas* (i.e., ideas travel from one locality to another; from one local idea to a different local idea). We add evidence to existing scholarship in privacy and security by using translation theory to explain how standards and regulations are adapted to discrete settings [3, 7, 26, 29, 36].

Further, we make an original contribution to translation theory itself [6], *by illustrating the diverse range of entities that can comprise localities*. We also contribute to literature on information security and privacy standards. For example Backhouse, Hsu and Silva [4] discovered the various political, social, and economic forces that played a role in the creation of important standards. We go further in showing how translation is at play in local adaptations of these standards and how organizations like HealthEx must find ways to manage those translations or face losing the participants who fund the HIE. The forces in these localities may be diverse and parochial, but they play an equally important role as dispersed translators who decide what those standards mean in situ. We also contribute to the work in international standards *setting and execution*. Inevitably, standards will not operate unless myriad localities are socially motivated to invest resources in making the necessary translations. Otherwise the social and economic expenses needed to create such standards [25] are made waste.

Our contribution to practice is a better understanding of the local factors driving translation that organizations can leverage to influence the translation process. Factors driving translation include economic constraints, politics, conceptions of individual rights, interpretations of codified ideas, operational or functional efficiencies, organizational preferences, governance and leadership. For example, when HealthEx initially developed their privacy policies, individuals from across the state's healthcare community were invited to gather a range of views regarding health data privacy, while taking into consideration organizational preferences and functional efficiencies of operationalizing the policies. Governance came into play during the iterative evaluation of the organization's privacy policies. The role of leadership was recognized in the hiring of the external consultant whose expertise would enable a correct translation of HIPAA. There is rich opportunity for further examination of the role of these factors in regulation and policy development.

This research also highlights how the translation of policy through local knowledge can not only help an organization improve its key performance indicators, such as quality of care at the local level, but also provide a better understanding of general global regulations and their broader impact [22, 32]. This paper creates several opportunities for further research. First, additional research is needed to learn if privacy ideas travel under equivalent translations in contexts other than healthcare (e.g., banking, finance, retail). Second, we have been concerned only with information privacy standards. Future research could examine standards dealing with broader issues, such as information security in general (e.g., ISO/IEC 27002). Third, we limited our examination of privacy standards to the study of consent. It would be beneficial to investigate whether similar layers and localities affect other privacy constructs. Future research can also examine the application of translation theory in areas such as Internet of Things, where current privacy regulations are fairly coarse-grained.

## 7. Conclusion

Increasing dependence on technology has resulted in the need to effectively manage the privacy of the proliferation of online personal information. More than 200 different information security methods and standards have been identified in the literature pointing to the need for standardization. Despite the efforts to develop universally applicable privacy standards, it is recognized that standards need to be adapted to local settings to address local constraints and to ensure compliance with local regulations. The purpose of this paper is to explain how the implementation of privacy standards and regulations, emerges both differently and extensively in organizational privacy and security policies as privacy ideas travel across localities and how those translations can be managed. We assess privacy regulations by tracing the travel of policy ideas from the localities where regulatory agencies pronounce principles and legislation to the localities that develop and implement the policies for health data sharing. Our findings demonstrate that the translation of ideas result in a wide difference between the original global concepts to their ultimate local enactment. From a practical standpoint, this implies a recognition of the interpretive aspect of the development and execution of privacy policies in the organizational context. The application of translation theory to information privacy policy would be relevant to practitioners, especially in those countries, or industries where privacy regulation is not only sector-specific but also specific to the type of data being collected.

## 8. References

[1] M. S. Ackerman, "Privacy in pervasive environments: next generation labeling protocols", Personal and Ubiquitous Computing, 8 (2004), pp. 430-439.

[2] C. M. Angst, E. S. Block, J. D'arcy and K. Kelley, "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches", MIS Quarterly, 41 (2017), pp. 893-916.

[3] M. Aubry, "The social reality of organisational project management at the interface between networks and hierarchy", International Journal of Managing Projects in Business, 4 (2011), pp. 436-457.

[4] J. Backhouse, C. W. Hsu and L. Silva, "Circuits of power in creating de jure standards: Shaping an international information systems security standard", MIS Quarterly, 30 (2006), pp. 413-438.
[5] W. E. D. Creed, M. A. Scully and J. R. Austin, "Clothes make the person? The tailoring of legitimating accounts and the social construction of identity", Organization Science, 13 (2002), pp. 475-496.
[6] B. Czarniawska and B. Joerges, *Travels of ideas*, in B. Czarniawska and G. Sevón, eds., *Translating organizational change*, Walter de Gruyter, Berlin, 1996, pp. 13-47.
[7] R. Demir and D. Fjellström, "Translation of relational practices in an MNC subsidiary: Symmetrical, asymmetrical and substitutive strategies", Asian Business & Management, 11 (2012), pp. 369-393.
[8] H. Doorewaard and M. Van Bijsterveld, "The Osmosis of Ideas: An Analysis of the Integrated Approach to IT Management from a Translation Theory Perspective", Organization, 8 (2001), pp. 55-76.
[9] K. B. Eden, A. M. Totten, S. Z. Kassakian, P. N. Gorman, M. S. McDonagh, B. Devine, M. Pappas, M. Daeges, S. Woods and W. R. Hersh, "Barriers and facilitators to exchanging health information: a systematic review", International Journal of Medical Informatics, 88 (2016), pp. 44-51.
[10] J. L. Funk, "The co-evolution of technology and methods of standard setting: the case of the mobile phone industry", Journal of Evolutionary Economics, 19 (2009), pp. 73-93.
[11] T. Geller, "In Privacy Law, It's the U.S. vs. the World", Communications of the ACM, 59 (2016), pp. 21-23.
[12] A. Giddens, *The Consequence of Modernity*, Polity, Oxford, 1990.
[13] L. A. Gordon and M. P. Loeb, "The economics of information security investment", ACM Transactions on Information System Security, 5 (2002), pp. 438-457.
[14] K. E. Greenaway, Y. E. Chan and R. E. Crossler, "Company information privacy orientation: a conceptual framework", Information Systems Journal, 25 (2015), pp. 579-606.
[15] J.-P. Hubaux and A. Juels, "Privacy Is Dead, Long Live Privacy", Communications of the ACM, 59 (2016), pp. 39-41.
[16] A. Iyengar, A. Kundu and G. Pallis, "Healthcare Informatics and Privacy", IEEE Internet Computing, 22 (2018), pp. 29-31.
[17] M. Keil, E. H. Park and B. Ramesh, "Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle-blowing intentions", Information Systems Journal, 28 (2018), pp. 818-848.
[18] J. Kerr and K. Teng, "Cloud computing: Legal and privacy issues", Journal of Legal Issues and Cases in Business, 1 (2012), pp. 1-11.
[19] L. Kugler, "Online Privacy: Regional Differences", Communications of the ACM, 58 (2015), pp. 18-20.
[20] J. Lampel and H. Mintzberg, "Customizing customization", Sloan Management Review, 38 (1996), pp. 21-30.
[21] B. Latour and M. Callon, *Unscrewing the big Leviathan: How actors macrostructure reality and how sociologists help them to do so*, in K. Knorr-Cetina and A. V. Cicourel, eds., *Advances in social theory and methodology*, Routledge & Kegan Paul, Boston, 1981, pp. 277-303.
[22] M. Marshall, P. Pronovost and M. Dixon-Woods, "Promotion of improvement as a science", The Lancet, 381 (2013), pp. 419-421.
[23] J. Mason, *Qualitative Researching*, Sage Publications, London, 2002.
[24] M. B. Miles and A. M. Huberman, *Qualitative Data Analysis*, SAGE Publications, Thousand Oaks, CA, 1994.
[25] C. N. Murphy, "Voluntary Standard Setting: Drivers and Consequences", Ethics & International Affairs, 29 (2015), pp. 443-454.
[26] J. A. Nielsen, L. Mathiassen and S. Newell, "Theorization and translation in information technology institutionalization: evidence from Danish home care", MIS Quarterly, 38 (2014), pp. 165-186.
[27] OECD, *The OECD Privacy Framework*, Organisation for Economic Co-Operation and Development, Paris, 2013.
[28] B. Otjacques, P. Hitzelberger and F. Feltz, "Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing", Journal of Management Information Systems, 23 (2007), pp. 29-51.
[29] J. Pries-Heje and R. Baskerville, "The translation and adaptation of agile methods: A discourse of fragmentation and articulation ", Information Technology & People, 30 (2017), pp. 396-423.
[30] J. R. Reidenberg, "Resolving conflicting international data privacy rules in cyberspace", Stanford Law Review, 52 (2000), pp. 1315-1371.
[31] K. H. Rolland and E. Monteiro, "Balancing the local and the global in infrastructural information systems", The information society, 18 (2002), pp. 87-100.
[32] C. Sausman, E. Oborn and M. Barrett, "Policy translation through localisation: implementing national policy in the UK", Policy & Politics, 44 (2016), pp. 563-589.
[33] P. M. Schwartz, "The EU-US privacy collision: A turn to institutions and procedures", Harvard Law Review, 126 (2013), pp. 1966-2009.
[34] H. J. Smith, T. Dinev and H. Xu, "Information privacy research: an interdisciplinary review", MIS Quarterly, 35 (2011), pp. 989-1016.
[35] Z. Tang, Y. Hu and M. D. Smith, "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor", Journal of Management Information Systems, 24 (2008), pp. 153-173.
[36] A. Tatnall and J. Lepa, "The Internet, e-commerce and older people: An actor-network approach to researching reasons for adoption and use", Logistics Information Management, 16 (2003), pp. 56-63.
[37] J. R. Vest and L. D. Gamm, "Health information exchange: persistent challenges and new strategies", Journal of the American Medical Informatics Association, 17 (2010), pp. 288-294.
[38] R. K. Yin, *Case Study Research: Design and Methods*, Sage Publications Inc., Beverly Hills, CA, 2003.
[39] J. J. Young, "Separating the Political and Technical: Accounting Standard-Setting and Purification", Contemporary Accounting Research, 31 (2014), pp. 713-747.