Legal Limits of Metadata Use for the Ancillary Healthcare Marketplace

Written by
Gordon Bleil, MD

In partial fulfillment of the requirements for
MMI 407 DL - Winter 2011
Karen Lindgren, Esq.

Research Paper

Introduction

The pharmaceutical industry is constantly under scrutiny for its practices because it is such a profitable business. Any opportunity to limit its power is considered to be a ‘good thing’. Recently particular attention has been paid to its marketing practices and the use of metadata from pharmacy sales to improve detailed sales efforts. (Conn, 2007) The risk of this attention is that it might remove a valuable tool from the marketplace. Metadata provides information about what is being done and by whom, but avoids the issue of whom it is for. (McLean, Burton, Haller, & McLean, 2008) This is not Protected Health Information (PHI) as defined by the Health Information Portability and Accountability Act (HIPAA), (DHHS, 2011b), but when it is created as a result of PHI transactions it can have different ramifications. There are currently many different standards regarding the use of this data, depending on the venue. Legally defining the appropriate uses of this data, with ethical standards and social acceptance being the hallmarks of appropriateness, will help the industry to move forward with greater confidence and more defined risk.

The barriers that this ambiguity creates can be seen within the ancillary medical marketplace and Health Information Exchanges (HIEs). The drivers for change in these industries include physician workflow, patient safety, medicolegal risk, regulatory compliance, and informed consent. Compliance issues abound with HIPAA and routine business privacy requirements. Implementation of a legislative solution is likely to be challenged by the pharmaceutical industry since they do not want any restriction on the status quo and by providers who want to limit access to information about their practices. Because industry is divided, and the patient’s advocate by default is the government, it seems likely that a modification of the current oversight mechanisms for HIPAA would be used to monitor usage and provide penalty or corrections when needed.

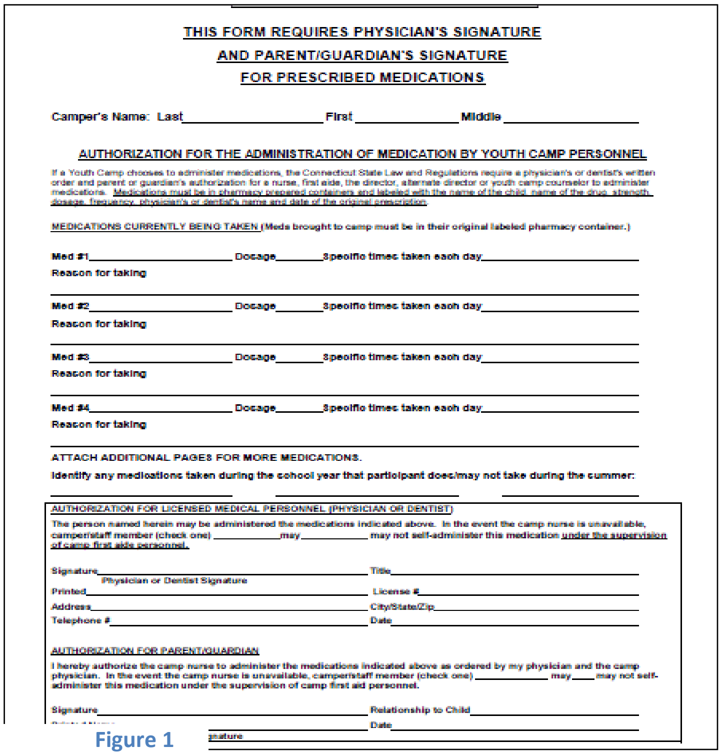
This paper discusses the legal issues regarding the commercial exchange of information between Covered Entities (CEs), such as medical providers and medical equipment vendors, and how the advent of improved legal guidance regarding the metadata from an 'intelligent' Electronic Data Exchange (EDI) might affect the patients, CEs, and the market from legal, ethical and social standpoints. Of particular concern would be whether utilization of 'intelligent' systems to gain information about medical transactions by CEs is a violation of the general concept of privacy, specifically would this be in compliance with the HIPAA rules. (DHHS, 2011b)

Current State

The present burden of documentation for ancillary healthcare products and services is not necessarily going to improve in the new HITECH environment. Each time a healthcare facility with an Electronic Health Record (EHR) receives or creates a document there is a risk that the document will not integrate well into the system. This lack of integration increases risk within the system. The details of this process highlight the drivers for change.

The costs of this burden go beyond the time fill out the forms. Reviewing documents occurs throughout the day and distracts the provider from the primary task of seeing patients. It is well known that distractions increase the risk of errors, and the greater the change in thought process, the greater the risk of error. (Ely, Levinson, Elder, Mainous, & Vinson, 1995; Reason, 1995) The consequences of error in medical care can be deadly, which has been one impetus for providers to delegate duties to staff who can provide the necessary attention to detail that these documents require. (Relman, 2001) In one study, the average physician saw 97 patients and handled 335 documents per week. (Shelagh McRae, 2006) A significant proportion of these exchanges of PHI include prescriptions of a drug, device or service. Insufficient information on the prescription is written will cause the vendor to contact the provider with a request for additional information in order to meet reporting the requirements of the vendor.

With each transaction providers need to review the data and return the requested information to the vendor in a usable format. The multiplicity of non-standardized formats vendors use exacerbates this problem. There are many examples of this – durable medical suppliers, oxygen/respiratory vendors, Hospice, school/camp physical forms (Figure. 1). Some prescriptions require ongoing documentation. Diabetic patients who monitor their blood sugar are given an initial prescription that includes the specific diagnosis and ICD-9 code (not a necessity for most prescriptions for drugs). In order to continue providing the device, the vendor is required to document that the provider is adequately monitoring the patients' use of the device and the benefit derived. In order to substantiate this



THIS FORM REQUIRES PHYSICIAN'S SIGNATURE
AND PARENT/GUARDIAN'S SIGNATURE
FOR PRESCRIBED MEDICATIONS

Camper's Name: Last__________ First __________ Middle __________

AUTHORIZATION FOR THE ADMINISTRATION OF MEDICATION BY YOUTH CAMP PERSONNEL

If a Youth Camp chooses to administer medications, the Connecticut State Law and Regulations require a physician's or dentist's written order and parent or guardian's authorization for a nurse, first aide, the director, alternate director or youth camp counselor to administer medications. Medications must be in pharmacy prepared containers and labeled with the name of the child, name of the drug, strength, dosage, frequency, physician's or dentist's name and date of the original prescription.

MEDICATIONS CURRENTLY BEING TAKEN (Meds brought to camp must be in their original labeled pharmacy container.)

Med #1__________ Dosage_____ Specific times taken each day__________
Reason for taking

Med #2__________ Dosage_____ Specific times taken each day__________
Reason for taking

Med #3__________ Dosage_____ Specific times taken each day__________
Reason for taking

Med #4__________ Dosage_____ Specific times taken each day__________
Reason for taking

ATTACH ADDITIONAL PAGES FOR MORE MEDICATIONS.

Identify any medications taken during the school year that participant does/may not take during the summer:

AUTHORIZATION FOR LICENSED MEDICAL PERSONNEL (PHYSICIAN OR DENTIST)

The person named herein may be administered the medications indicated above. In the event the camp nurse is unavailable, camper/staff member (check one) ________ may ________ may not self-administer this medication under the supervision of camp first aide personnel.

Signature__________ Title__________
Physician or Dentist Signature
Printed__________ License #__________
Address__________ City/State/Zip__________
Telephone #__________ Date__________

AUTHORIZATION FOR PARENT/GUARDIAN

I hereby authorize the camp nurse to administer the medications indicated above as ordered by my physician and the camp physician. In the event the camp nurse is unavailable, camper/staff member (check one) ________ may ____ may not self-administer this medication under the supervision of camp first aid personnel.

Signature__________ Relationship to Child__________
Date__________
gnature

Figure 1

request for continuation of service, records are requested that include blood testing every 3 months and at least annual office visits.   Providers with an EHR establish workflows that allow them to search the record, complete the form, and return it effectively. Often the result is a hybrid system of data storage, and each interfacing step represents an opportunity for lost data, translational error, transcriptional error, or delay.

There are currently EDIs that resolve similar issues with claims data, but the data sets are limited and highly standardized. The metadata that is generated by these agencies is not generally used for marketing purposes because of the limited data set and the greater value of the PHI that is transmitted between the CEs.   There are also Electronic Prescribing systems, but they also have a limited dataset. The metadata that is generated by these systems has been used for many years by pharmaceutical manufacturers to supply their salespeople with detailed information regarding the providers they call on.

HITECH Alternative

Within the HITECH environment, the ubiquity of information systems will allow for a higher level of automation. Utilizing the presence of the EHR the process would begin with the generation of an electronic data request. This would be transmitted to an EDI where the message would be translated and transmitted to a search engine and Clinical Decision Support (CDS) software to determine whether the necessary data is present within the provider's database. When the data is available, the system would complete the form, require the provider to review the form for correctness, and submit the form electronically. (Figure 2)   This combination of technology within a secure network, with provider approved information transmitted through an EDI could be described as an 'intelligent' system.

The Environment – EDIs and HIEs

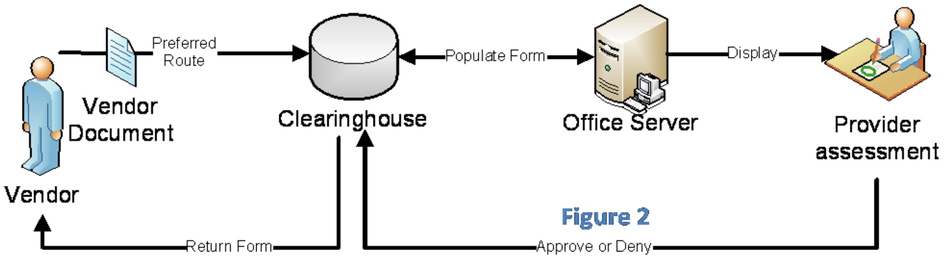


Figure 2

Use of an intelligent system is based in the concept of the EDI which is a derivative of the clearinghouse. Historically, clearinghouses were a physical location where bankers could meet to exchange checks and other items drawn on each other in order to settle accounts. (2008) Subsequent development of information systems began to implement repositories to collect, store, and disseminate information, metadata, and data. These commonly would provide widespread information access, reaching outside organizational boundaries. (Wikipedia, 2011a) This created HIPAA conflicts when information was being sent over the internet to insurance providers, so further developments created EDI entities to receive claim data, translate it to ANSI format, and forward it securely to other systems. (Wikipedia, 2011d)   The limited function of the EDI did not allow for collection, de-identification or aggregation of health information, limiting the value of the EDI toward improving healthcare.   It was merely a secure conduit to get information that providers and insurers could use to send very limited and pre-determined datasets to each other.

In describing this problem, the terms EDI and HIE have both been used.   A 'HIE is defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system.' (Wikipedia, 2011c) A HIE creates a pair of functional opportunities – the ability of accumulated PHI to be available upon authorized access from outside the organization that created it, and for de-identified data to be available for aggregation. With the EDI offering a conduit, and HIEs offering accumulated and aggregated data, the missing option is the ability to request very specific, variable data sets from a particular provider for the purpose of providing drugs, devices or services. This could be done with an HIE, but the vendor needs to send a request through the HIE or the provider, and the provider needs to certify the information. This substantially changes the primary goal of the HIE.

Legal Issues

In order to promote development of more automated systems for management of documents related to the ancillary healthcare market several issues need to be addressed. These include assuring a sustainable model for information exchange, physician workflow reduces the risk of error, patient safety is not compromised, medicolegal risk is mitigated, regulatory compliance is straightforward, and patients and providers are informed about the use of information so that they can appropriately consent to its use. Other issues include fraud and abuse, technical liabilities and defining the boundary where metadata begin to sufficiently emulate PHI or describe the activities of individuals (providers) in ways that invade their privacy.

System Issues

One of the challenges of HIE development has been the ability to develop a self sustaining financial model. Maintaining legally and ethically clean and clear access to PHI is the gauntlet laid by society. Any blurring of that line is likely to raise red flags. But attachment of EDI and potential market services based on aggregation of metadata could represent a new financing mechanism. Linking data regarding the provision of drugs, equipment and services to aggregated data from an HIE might also create an opportunity for better measurement of consumption and therefore fraud prevention. Creating a utility/monopoly requirement that prescriptions go through a HIE would go a long way toward creating a core value for the HIE in the battle to reduce the cost of healthcare. This makes for high stakes on both sides.

Metadata represent a space slightly to the side of PHI that might offer an option to appease both society and the business world. In addition to the risks associated with this biased data, the limited range of data points could result in skewed patient management if business choices are made based on data from only these reported elements. This could create inappropriate measures of 'success' based on completed reports with limited information, leading to amplification of process changes that move away from good patient care. Keeping the data sets standardized based on best practices will help to mitigate this effect. This creates a potential benefit of linking the results of metadata analysis to aggregation of de-identified data from an HIE. The intermediary has the potential of being relied on to provide the 'correct' standards for vendors and practices. Although the EDI would be an expert, it would remain incumbent upon all parties to assure that they are not misled into litigation. Centralizing the process could also overtly or inadvertently encourage providers and/or vendors to 'play the reimbursement game' and pay less attention to patient needs. This focus on business instead of patients is what sets the stage for fraud and abuse.

Fraud has always been a concern to the Federal government, but in recent years it has become a hotbed of action, making it a particular concern to providers and vendors alike. The inclusion of CDS into the intelligent EDI system offers the opportunity for fraud prevention on two levels. Introduction of a 3rd party into any interaction, especially one that has legitimate interests to maintain, decreases the risk of fraud. Allowing the 3rd party to be a part of the decision making process, helping to set the rules for transmission of data across the network, further decreases the risk of overt and covert fraud. The remaining risk is that of inadvertent fraud, which is reduced by having more than one party involved in the decision making process.

A final concern would be the extent to which combining the HIE and EDI would create anti-trust concerns. This would create an opportunity to control information and therefore control some elements of the marketplace. This issue would need to be fully considered with each aspect of the data association process.

Data Mining

Data mining is a process during which large data sets are searched so that patterns can be discerned based on combined methods using statistics and artificial intelligence with database management. (Wikipedia, 2011b) In comparison, analysis and searching of a providers' database for the purpose of providing required support to an individual's prescription is a directed query rather than mining.

Using data mining methods on PHI, as opposed to metadata obtained from PHI transactions, yields very different information. Mined identifiable patient information is still protected. Mined metadata is nominally not identifiable and could be used to transform data into business intelligence giving an informational advantage. Recent court rulings seem to support that metadata is part of the public domain, at least from government sources. (Millonzi, 2011) These methods are currently used in other ways for profiling practices, such as marketing and fraud detection. This process might employ evaluation of smaller samples to generate questions for investigation by using *data dredging*, *data fishing* and *data snooping* on the metadata set.

As noted, metadata is not PHI, but is extremely valuable as a marketing tool. The number of prescriptions from a particular provider (or specialty, or area) to a particular vendor (or type of device) might be a particularly useful tool for vendors. This data might also be of use to look at utilization of methods, of vendors, or regarding persistence of use when compared to aggregated information from an HIE regarding the prevalence of a particular disease for which prescriptions are written. One caveat to this carte blanche allowance for using metadata is if mining results in a data set that models the original PHI. If this occurs to a sufficient degree, release of that new data set could be considered a breach of HIPAA. Additionally, the metadata model may create an unacceptable view of the providers practice and create controversy at best, liability at worst. If the model was modified, with PHI data kept by the EDI, it would be possible for the intermediary to aggregate de-identified data. That would further allow the metadata to be 'matched' to the aggregated data for further analysis. Under those conditions it would likely be difficult for an outsider to discern the difference between an HIE and an EDI.

The EDI intermediary is likely to keep track of the type and level of transactions for their own business intelligence. It is not clear what restrictions there are on how that information can be developed, used or sold. In recent years that has been much analysis of the pharmaceutical industries use of sales data from pharmacies, but there is very little case law to define the boundaries of use. There has been concern about the risk to patient's privacy (Conn, 2007), and to physician privacy. (Sibbald, 2003)

With these important differences between HIEs and EDIs identified, it is of key importance to identifying the character and source of the data when attempting to determine whether it is legally and ethically appropriate to mine it. This in turn can be critical to creating an environment in which consumers (providers and patients) feel that mining is socially acceptable.

Technical Liability Issues

Administrative Simplification requires that Covered Entities use designated standard transaction formats and code sets for the electronic transmission of health information, and establishes standards for the privacy and security of individually identifiable health information, and provides penalties for its wrongful disclosure. (Office of the Secretary, 2006) An EDI requires a business model with interfaces between each vendor and each provider. This interface engine would utilize many current standards, although at least one potentially useful standard (Virtual Medical Record) is still in development. The legal risks associated with any interface engine are primarily related to incorrect translation of data, or transmission to the wrong party. This is a greater risk with new technology. Well established coding standards such as SNOWMED-CT, ICD-9, and CPT create more endpoint interpretation risks. The requirement to transition to ICD-10 in 2013 may create some technical, translational risks, but again will be more likely interpretation risks not borne by the EDI.

The CDS standards are HL7 based and include Arden Syntax**,** Virtual Medical Record (VMR), GELLO, Infobutton (request and response), Decision Support Service, and Order Set. Not all of these are fully developed, but when VMR standard is released it is likely to substantially improve the capability of decision support programs to move into other systems easily. (Howard R. Strasberg, 2011) Simplifying and enhancing the development of information exchanges will be an important step in reducing risk. CDS rules developed may be an opportunity to create patentable intellectual property, but most of the system would be created from ‘off the shelf’ technology. The level of efficiency created by the CDS rules would represent the marketable margin.

Provider Issues

The benefits and risks of developing a better legal definition for the acceptable use of metadata will be most obvious to providers. Improved workflow is a paramount concern, with the need to meet legal and reporting requirements close behind. The cost of implementation and maintenance will be considered in the balance. The balancing concern would be the risk of vendors knowing more about the providers practice.

Within the current workflow it is possible for a prescription to begin with a vendor, the patient or the provider. In all cases the request is funneled through the provider, creating a bottle neck which slows the process. Because of the amount of manual intervention required to complete this task, it is common that the forms are incompletely filled out, the data is inaccurate, and the ‘extra effort’ to pull data from the chart puts the task low on the priority list. Each time the process is pushed away from the provider, the risk of inaccuracy is increased.

Historically there have been several approaches to relieve this bottle neck. The nursing profession and other ancillary services have been authorized to write Verbal Orders to be later cosigned by the physician. The relatively new Midlevel providers (Nurse Midwives, Nurse Practitioners, Nurse Anesthetists, and Physician Assistants) can write many prescriptions without the need for co-signature. Use of signature stamps is allowable for some prescriptions and other documents. Recently there has been an attempt to restrict certain high fraud level prescriptions by requiring original signatures of physicians. ("CR 5971 Clarification - Signature

Requirements," 2008) This is being mitigated by the acceptance of electronic signatures, but it still creates an increased burden on the provider since staff cannot perform the task.

CEs are allowed to freely exchange PHI with other CEs or partners with whom they have a BAA as long as it is part of business operations. The result is that each vendor or provider tends to create their own form or standard based on the interaction. There is no direct reimbursement to the partner in these circumstances, and CMS has no real interest or jurisdiction over the data request. The transaction must still use standard language, but not necessarily a standard data set. An insurance company, for example, may send a request to the provider to change a patient from a non-formulary drug to one on the formulary. The driver in this case is peer pressure to lower the cost of care and the minimum necessary data set is established by the vendor, but similar examples exist where providers are the demanding partner.

Hybrid systems represent a particular risk to information systems. (Borycki & Lemieux-Charles, 2008; Dimick, 2008; Hamilton, Round, Sharp, & Peters, 2003) With both paper and electronic formats, it is difficult to maintain an effective scanning and image storage system efficiently. Indexing is typically a manual process, with high cost and risk of mislabeling objects. Lack of consistency between indexing staff, failure to recognize format or information, and inappropriate levels of indexing (either too much or too little) can result in effectively lost images. There are also typically limits on cross indexing, leading to inadequate searching capabilities. Optical character recognition can lead to a different and equally challenging set of risks. The data could alternatively be entered into the electronic system manually, but this increases the risk of incomplete information, translational errors, and loss of the original image as a source of information. Utilizing electronic formats with discrete data sent through the interface engine would allow the data to be placed where it can be optimally utilized, decreasing the risk of functional loss. Recently vendors have been setting up web access to allow providers to do this work electronically, but this does not integrate with the electronic record and requires the user to access a web site outside the office to accomplish the work. This is only a gain for the vendor.

Allowing forms to be prefilled for provider would allow the complete dataset to be put in front of the provider for approval immediately. If missing data is noted the office staff can arrange for the patient to get the appropriate office visit and/or testing done in order to complete the data set. Since the CDS rules would be set up by the EDI using the criteria of the provider and the vendor, using the intelligent EDI will improve the clarity and quality of required datasets. User involvement is the most effective approach to help providers to feel comfortable with this support system. Using a stepped approach to dataset development with information coming from a snapshot of the data followed by active approval of the provider before transmission, maintains control of the data within the practice but there is no direct link to the active dataset. The resulting approved data would then be incorporated into the active data set. This added element of security would prevent the system from being able to make uncontrolled or unsynchronized changes to the active dataset.

Vendor Issues

Currently vendors send out requests for data and hope that they get returned. There is a 30 day window, for example, that Homecare Agencies have to get their initial assessment and care plan returned from the authorizing provider. Failure to meet this deadline can mean that the vendor does not get paid. There is a strong motivation for the vendor to push the provider, or to send in fraudulently completed documents. It would clearly be an advantage for vendors to get reports back faster with consistently correct and complete information based on the decision support rules set up for the system. The appropriate CPT, ICD-9/10 and other codes are provided, not just common language diagnosis with its inherently increased risk of misinterpretation. An electronic system would also be able to be queried regarding the status of a request, or reports could be sent back to the vendor at standard times. If there is a delay in order to complete labs or an office visit the vendor is not left in limbo. Overall an automated process would help to minimize turnaround times and improve business relations.

Patient Acceptance

Patients have the least concern with the present system, but that is likely more of a problem than a benefit. Lack of patient awareness and understanding about what happens after the patient encounter, when the prescription is accepted and passed on to the vendor, encourages business to keep the process quiet but lucrative. An EDI approach offers benefit to the patient who is concerned about what happens with information obtained from their use of the healthcare system. A more direct benefit would be rapid turnaround to increase the potential for early reimbursement. Clean and complete datasets help set the stage for more effective measurement of health status and progress.

The patient has traditionally been passive in this process, but the advent of patient centered care, as recommended by the IOM, will likely increase the interest of patient in what permissions they tacitly provide when accepting a prescription. (Relman, 2001) These permissions allow others to move, record, analyze, and report data regarding health transactions that affect their future health care opportunities. The classic advertising case of this circumstance is when checks are sent out which the unwitting consumer cashes. On the check it states that by depositing this check they agree to the terms and conditions of the marketer. Patients don’t have that caveat imprinted onto the prescription that they submit to a vendor. If patients are empowered to seek this knowledge, it will be interesting to see how long they remain willing to accept a prescription that allows permission to share metadata related to the transaction. There is no substantial evidence that public perception of data aggregation for the purpose of market analysis is a problem. It is being used extensively with web page advertising and has had no significant backlash. There are grumblings about invasion of privacy when people realize that the web advertising they are seeing is not the same as their neighbors, but for the most part they either ignore it or find it helpful.

The authority provided by prescription is specifically to allow the vendor to supply the patient based on the written instructions of the provider. In most cases the patient has concern about whether the drug, device or service will be covered by their 3rd party payer and/or if the therapy is indicated and helpful. There is generally an assumption that a prescription will be written, the vendor will supply it, and the only the provider, vendor and 3rd party payer will be knowledgeable about the transaction. Whether the vendor keeps track of which providers prescribe that service, or then number of times it has been prescribed in area code 40404 is market data and not usually a worry for patients. On the other hand, market data used to send out coupons or special sale information based on which pharmacy customers picked up over the counter urine test strips used for diabetes is not a concern for patients either. Yet this information is patient specific and associates the patient with a disease. In this complex environment the goal of maintaining patient privacy is challenging. Patients seem have a clear expectation about privacy of the information elicited from provider encounters and a willingness to accept electronic data sharing as long as those expectations are met (Chhanabhai & Holt, 2007), but it still remains unclear what level of understanding patients have about the permissions they tacitly provide when accepting a prescription. The same would be true for providers when they write a prescription. Clearly neither party was highly aware of this issue until it became more public knowledge that pharmaceutical companies were buying prescription sales information from pharmacies.

These elements of legal and ethical concerns about information sharing aside, there are other significant risks in the current prescription system. It was most common 25 years ago that all prescriptions were filled by local vendors. There was a rather loose system of signature verification based on being known in the community. With the advent of pharmacy benefit providers, standalone services providers, increased travel, and Web based businesses the methods of verification have changed. It is still acceptable to be 'known in the community' or to verify by phone call under certain conditions, but a more common method is by verification of personal identifiers including Universal Provider Identification Numbers (UPIN) and Federal Drug Enforcement Agency (DEA) numbers along with procurement of contact information through independent sources (e.g. phone book, web site, patient provided information). There are also social and ethical evaluations done by vendors based on the provider knowledge of the language, and familiarity with the disease and prescription when discussing it with them on the phone.

A part of the process of verification is also the information trail. With prescriptions written on paper, these papers need to be stored or imaged in order to be able to provide verification of authority information later on. Storage and retrieval of prescription information is cumbersome. If there is an associated electronic medical record, imaging storage issues will persist. Electronic systems, using metadata, offer a substantial trail to follow.

The value of having more data analysis being done by the computer would result not just from the potential to reduce total volume by careful association of indications to prescriptions, but there is also the potential to monitor changes in condition by polling for changes in dataset. This method of data monitoring was commonly used to assure that parallel databases were synchronized, but would offer an option for catching changes to the database as well.

Compliance

HIPAA violations are a more recent concern in healthcare. Providers are compelled to transmit information to vendors, lack knowledge about what the minimum data requirements of the vendor or other CE really are. The HIPAA rules allow this ambiguity by assuming that either the BAA will define this, or if the exchange is with another CE, that the CE is responsible to demonstrate that they have a need for the data when audited. The process of using an 'intelligent' EDI would alter the ability of the provider to be aware of what the minimum data needs of the vendor.

Once held by the CE or Business Associate (BA), use of the data and metadata that providers transmit is not governed, with the caveat that PHI cannot be transmitted beyond the scope of the BAA. Patients especially are currently unaware of the extent to the permissions that are created with the acceptance of a prescription that allow others to move, record, analyze, and report data regarding health transactions. Public perception of data aggregation and data sharing are at best incomplete.

The industry limits for communication of PHI are established by the government agencies that are going to use the data and those that protect patients from harm. The range of acceptable PHI data transference is extremely narrow from a theoretical legal perspective, but very broad from a functional perspective. The ability of information to be shared for operational needs is very broad and commonly encompasses much of the additional information transmitted. The HIPAA established the Minimum Necessary rule. This rule states that only the minimum amount of data necessary for each healthcare transaction should be communicated between CEs, but this amount is determined by the requesting party. If a violation is found then the Centers for Medicare & Medicaid Services (CMS) has the authority to penalize the offending parties with monetary fines and the inability to participate in Medicare and Medicaid programs. This penalty is by far the greatest risk to medical businesses and the driver to keep them compliant.

The legal standards set by HIPAA include specific definitions of PHI and when BAAs are required. In this model, there would be agreements between the intermediary EDI and every provider or vendor. Third parties are allowed to share PHI as specified in a BAA, although in this case the situation is modified because 2 different 3rd parties work ‘outside’ of the patient care environment. (DHHS, 2011a) Compliance would be monitored in the same way that HIPAA currently is, based on patient complaint or CE reporting. The system is set up to allow for limitation of penalty based on self reporting so long as the CE follows process elements set forth under the Federal Sentencing Guidelines. It would be optimal ethically, but perhaps not socially acceptable (i.e. not marketable) to include information about the potential use of metadata about transactions in which the provider and vender were involved. General privacy rules and disclosure of business practices would govern these decisions. Keeping the ideal of confidential information, not just the legal requirements of privacy, at the forefront of this process is important. This was well stated by Richards and Solove in their article on privacy: ‘Confidentiality is thus a key dimension of privacy; it cannot be excised from privacy nor can it serve as the sum and substance of privacy either. Because they protect distinct dimensions of the ways in which unwanted disclosures of personal information can be harmful, both confidence and American-style privacy are worth protecting’. (Solove, 2007)

An interesting opportunity might arise if there were appropriate BAAs in place. If the EDI keeps a copy of the data that flows through there would be an opportunity to de-identify and aggregate the data. Once de-identified, aggregated or not, the Privacy Rule no longer applies to transactions of the data. (NIH, 2007) This would clearly be a skewed set, biased by the requirement that the data was related to the prescription of a drug, device or service. This would represent a key difference between the results of studies done on the data, but an outsider be have a great deal of difficulty discerning any other difference between the EDI and an HIE.

Proposal

Each of the issues presented describes the current problems faced by the stakeholder, the legal issues of concern, and the changes to be brought about by technology. The legal, ethical and social risks and benefits of these changes follow. Currently states are individually trying to set the standard for their citizens regarding the use of PHI metadata analysis for business purposes, but the Federal government is setting standards for PHI, pharmaceutical business, and promoting the HITECH environment. It would be appropriate and helpful to develop Federal standards for PHI metadata analysis that clarify the boundary between private and public allowable use. This boundary can be defined based on current standards of privacy and confidentiality, using the hallmark of identifiability. So long as the metadata are not analyzed in a manner that creates a record that can reasonably pinpoint an individual or their habits then its use would be acceptable. Federal law is needed due to the ability of electronic systems to be blind to political boundaries and to increase the potential that international conflicts can be negotiated more effectively. Federal law is more likely to be helpful in prosecuting fraud and abuse and use of metadata may be particularly helpful in these cases.

Summary

Creating new Federal law that would allow for clear distinction of the boundary between private and public use of metadata would promote the development of EDIs that could assure provider workflow is improved, patient safety is not compromised, medicolegal risk is mitigated, regulatory compliance is straightforward, and patients and providers are informed about the use of information so that they can appropriately consent to its use. Defining this boundary might also help EDIs to work more closely with HIEs reduce the cost of healthcare through better marketing as well as reductions in fraud and abuse. These benefits would accrue by legally limiting the analysis of metadata to prevent emulation of PHI, or describe the activities of individuals (providers) in ways that invade their privacy.

Assuming a distinction is made between an EDI and a HIE using the functional elements of intent and storage of data, it would be possible to create an intelligent EDI to semi-automate the process of communicating with providers. This analysis and searching of a providers' database for the purpose of providing required support to an individual's prescription does not represent data mining.

With appropriate Business Associate agreements (BAA) in place, and the PHI passed through the EDI but not recorded, the intermediary could keep track of the type and level of transactions in order to aggregate marketing data for the vendors. There may be some restrictions on how the information will be developed, used or sold, but those restrictions are not yet developed. They will likely come out of the pharmaceutical companies drive to preserve the market information they get from pharmacies.

If the data is kept by the intermediary EDI, there would be greater question about whether it would be allowable to aggregate de-identified data for vendor use. Where de-identification has not been consistently helpful for medical research (Gellman, 2010), marketing research is not only less rigorous, but also looks for different results. If the EDI begins to store and analyze health information directly it would be less obvious to an outsider that there is a difference between a HIE and a EDI. Indeed, that may segue into a new model for HIE financing.

The process of using an 'intelligent' EDI will not likely help to create standard by which the provider could know what the minimum data set is for a given vendor. With this potential lack of clarity, the providers will find it helpful to have support in supplying information to vendors. Workflow is the primary driver for providers, with meeting legal and financial requirements close behind.

Patients would not likely have any better understanding about the permissions they tacitly provide when they accept a prescription, but they are likely to become more aware of the extent to which these permissions allow others to move, record, analyze, and report data regarding health transactions. The patients' willingness to accept a prescription may be affected if they are unsure what permissions to share information they are allowing. The public perception about using data aggregation for the purpose of market analysis remains unsettled, but likely this will become an increasingly difficult battle.

As development and implementation of the HITECH environment continues, it will be interesting to explore the ramifications of these connections. With multiple relationships being created by the EDI (or with the NHIN), it could well be that the socially notable '6 degrees of separation' will come into play between medical data sources. That is likely to be both a useful and dangerous relationship. The more we can clarify the boundaries of private and public use of information, the greater the potential that we will be able to manage that kind of exponential growth.

Bibliography

(2008, 2008) Retrieved March 5, 2011, from www.investmentsandincome.com/banks-banking/banking_terms.html

Borycki, E. M., & Lemieux-Charles, L. (2008). Does a hybrid electronic-paper environment impact on health professional information seeking? [Comparative Study
Randomized Controlled Trial]. *Studies in Health Technology & Informatics, 136*, 505-510.

Chhanabhai, P., & Holt, A. (2007). Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. [Comparative Study]. *Medgenmed [Computer File]: Medscape General Medicine, 9*(1), 8.

Conn, J. (2007). State loses data-mining case. N.H. plans appeal of ruling allowing use of Rx data. [Legal Cases]. *Modern Healthcare, 37*(20), 32.

CR 5971 Clarification - Signature Requirements. (2008). Retrieved from http://www.ois-inc.net/MLNMatters%20CR%205971.pdf

DHHS. (2011a). Collection, Use and Disclosure Limitation. *The HIPAA Privacy Rule and Electronic Health Information Exchange in a Networked Environment* Retrieved March 1, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/collectionusedisclosure.pdf

DHHS. (2011b). Health Information Privacy Retrieved 3/6/2011, 2011, from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

Dimick, C. (2008). Record limbo. Hybrid systems add burden and risk to data reporting. *Journal of Ahima, 79*(11), 28-32.

Ely, J. W., Levinson, W., Elder, N. C., Mainous, A. G., 3rd, & Vinson, D. C. (1995). Perceived causes of family physicians' errors. [Research Support, Non-U.S. Gov't]. *Journal of Family Practice, 40*(4), 337-344.

Gellman, R. (2010). Why deidentification fails research subjects and researchers. [Comment]. *American Journal of Bioethics, 10*(9), 28-30.

Hamilton, W. T., Round, A. P., Sharp, D., & Peters, T. J. (2003). The quality of record keeping in primary care: a comparison of computerised, paper and hybrid systems. [Comparative Study
Multicenter Study
Research Support, Non-U.S. Gov't]. *British Journal of General Practice, 53*(497), 929-933; discussion 933.

Howard R. Strasberg, M., MS. (2011, 2/23/11). *Clinical Decision Support Standards* Paper presented at the HIMSS11, Orlando, FL.

McLean, T. R., Burton, L., Haller, C. C., & McLean, P. B. (2008). Electronic medical record metadata: uses and liability. *Journal of the American College of Surgeons, 206*(3), 405-411.

Millonzi, K. (2011, March 4). Is Metadata a Public Record? An Analysis Under Federal FOIA. Retrieved from http://sogweb.sog.unc.edu/blogs/localgovt/?p=4023

NIH. (2007, 2/2/2007). How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule? *HIPAA Privacy Rule - Information for Researchers* Retrieved March 1, 2011, from http://privacyruleandresearch.nih.gov/pr_08.asp

Office of the Secretary, H. H. S. (2006). HIPAA administrative simplification: enforcement. Final rule. *Federal Register, 71*(32), 8389-8433.

Reason, J. (1995). Understanding adverse events: human factors. *Quality in Health Care, 4*(2), 80-89.

Relman, A. S. (2001). The Institute of Medicine Report on The Quality of Health Care Crossing the Quality Chasm: A New Health System for the 21st Century. By the Committee on Quality of Health Care in America of the Institute of Medicine. 337 pp. Washington, D.C., National Academy Press, 2001. $44.95. ISBN 0-309-07280-8. *New England Journal of Medicine, 345*(9), 702-703.

Shelagh McRae, M., CCFP, FCFP and Robert Hamilton, MD. (2006). The burden of paperwork. *Can Fam Physician, 52*(5), 586–588.

Sibbald, B. (2003). Dispute over use of MDs' prescribing information heading to court. [Legal Cases News]. *CMAJ Canadian Medical Association Journal, 168*(3), 325.

Solove, N. M. R. D. J. (2007). Privacy's Other Path: Recovering the Law of Confidentiality. [Review article]. *Georgetown Law Journal, 96*(124).

Wikipedia. (2011a, 26 November 2010). Clearinghouse Retrieved March 5, 2011, from http://en.wikipedia.org/wiki/Clearinghouse_(GIS)

Wikipedia. (2011b, 4 March 2011). Data Mining Retrieved March 5, 2011, from http://en.wikipedia.org/wiki/Data_mining

Wikipedia. (2011c, 2 March 2011). Health Information Exchange Retrieved March 5, 2011, from HTTP://en.wikipedia.org/wiki/Health_information_exchange

Wikipedia. (2011d, 10 February 2011). Practice Management Software Retrieved March 3, 2011, from http://en.wikipedia.org/wiki/Practice_management