Crime and Punishment

Can the NHIN Reduce the Cost of Healthcare Fraud?

By Stephen T. Parente, PhD; Karen Mandelbaum, JD; Susan P. Hanson, MBA, RHIA, FAHIMA; Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS; and Donald W. Simborg, MD

KEYWORDS

NHIN, healthcare fraud, IT infrastructure, cost/benefit analysis, healthcare transactions.

ABSTRACT

In his 2004 State of the Union Address, President Bush called for the adoption of the electronic health record (EHR) to increase efficiency and improve the quality of healthcare. This system could reduce healthcare costs by 20 percent or more per year. Some of those savings would be attributed to a dramatic reduction in losses due to fraud. Though IT by itself cannot solve the problem of healthcare fraud, developing an interoperable National Health Information Network (NHIN) can provide a platform to implement real-time anti-fraud controls. In this paper we inventory the costs and benefits of fraud detection from the NHIN and conclude that such an infrastructure investment has the potential to produce significant national savings.

Healthcare fraud is a serious nationwide crime linked directly to the ever-growing annual US healthcare outlay. Although fraudulent transactions constitute only a small fraction of the more than four billion health insurance transactions processed in the United States each year, those fraudulent claims carry a high price tag.

"Estimates of annual losses to fraud range from 3 percent to 10 percent of national healthcare expenditures. This translates to $51 billion to $170 billion based on 2004 expenditures of $1.794 trillion. In comparison, credit card fraud, which is perceived as a huge problem, amounts to only $788 million in annual losses," according to a 2005 article in *Information Week*.[1]

"CMS projects national health expenditures to reach $3.6 trillion in 2014, growing at an average annual rate of 7.1 percent during the forecast period from 2003 to 2014. As a share of gross domestic product, health spending is projected to reach 18.7 percent by 2014, up from its 2003 level of 15.3 percent. One of the most significant events impacting the projections is the... Medicare Part D prescription drug benefit mandated in the Medicare Modernization Act."[2] It is not surprising that criminals view healthcare fraud as a lucrative field for illicit profit.

Since healthcare fraud may cost taxpayers as much as $170 billion a year, federal and state agencies have made prosecution for these crimes a primary focus. In 2001, the federal government won or negotiated more than $1.7 billion in judgments, settlements and administrative impositions in healthcare fraud cases and proceedings. In addition, the number of healthcare fraud cases referred for criminal prosecution by HHS has significantly increased. Though this represents the largest return to the government since the inception of the Health Care Fraud and Abuse program established by HIPAA in 1996, it is only a small fraction of expected fraud losses.

Fraud can be detected and reduced through a variety of IT capa-

bilities, including abnormal pattern recognition, system audits, practice pattern monitoring and controlled substance tracking. Other sectors of the economy, such as the credit card industry, have harnessed the power of technology to reduce fraud. "Credit card fraud has been reduced to about 7 cents out of every $100 spent on using cards," according to the *Washington Post*.[3] Much of the success in detecting credit card fraud is attributed to technology's effective recognition of spending patterns.

Fraud schemes range from those perpetrated by individuals acting alone to broad-based activities by institutions or groups of individuals, sometimes employing sophisticated telemarketing and other promotional techniques to lure consumers into serving as the unwitting tools in their schemes. Perpetrators seldom target only one insurer or either the public or private sector exclusively. Rather, most schemes attempt to defraud several victims in both the private and public sector simultaneously.

BACKGROUND

A National Health Information Network (NHIN) will offer new opportunities to detect fraud as well as identify new areas vulnerable to fraud. Though IT introduces predictability—which has the potential to enable fraud—systems can be programmed to detect suspicious behavior and prevent fraud from occurring.

The current health IT infrastructure consists mainly of stand-alone health insurer and medical providers systems, each attempting to address fraud from their own perspective. The interoperable system envisioned in the health IT strategic framework represents an efficient alternative to the current fractured system.[4] When interoperability is achieved, the benefits of developing the NHIN will outweigh the costs. Therefore, undertaking a rigorous economic analysis of the costs and benefits that compares the current prevention and detection capabilities to those that can be appreciated under expanded IT capabilities will shed light on the net value of the NHIN.

This study presents one of the first comprehensive analyses that tallies the costs and benefits associated with fraud-related activities in the healthcare sector. We contemplate the possibilities under four different interoperability scenarios. The methods used invoke a standard cost/benefit analysis; all impacts are relayed in monetary dollar units. The model evokes the discipline of economics by recognizing that losses that are incurred as a result of fraud are non-recoverable costs to society that do not provide benefit to either consumers or producers/providers in a market economy.[5]

PRINCIPLE RESEARCH QUESTION

At present, the cost of healthcare fraud per year could be tens of billions of dollars.[6] As we move forward, detection strategies must be strengthened and efforts to prevent fraud from occurring will be needed. The playing field of fraudulent activity is constantly changing. Therefore, maintaining effective fraud management tools demands continuous re-assessment of emerging fraud trends and constant revision of controls.[7]

A new health IT infrastructure will increase the speed of all healthcare transactions, both fraudulent and legitimate. Therefore, it is prudent to examine the costs and benefits of fraud detection and prevention under the different future IT development scenarios. As a result, the principle research question is: What is the expected fraud/non-fraud related cost/benefit associated with developing and implementing the NHIN with interoperable EHRs?

To answer this question, estimated fraud- and non-fraud-related costs and benefits were inventoried and tallied separately. On the costs side, fraud-related expenses include the resources currently lost due to various types of fraud, including but not limited to, identity theft, and seeking reimbursement for fake or feigned services. They also include the costs associated with investigating crimes, tracking down perpetrators and prosecuting offenders.

New methods to detect and prevent fraud are dependent upon new technology platforms. The non-fraud-related costs associated with the initial capital investment and the ongoing operating expenses of maintaining and increasing the interoperability of the IT systems that uncover the fraud represent the highest barrier to adoption.

Fraud can be detected and reduced through a variety of information technology capabilities, including abnormal pattern recognition, powerful system audits, practice pattern monitoring and tracking of controlled substances.

Fraud-related benefits include the recovery of the healthcare monetary resources lost due to bogus claims made by impersonators, as well as settlement agreements negotiated with practitioners. The non-fraud related benefits include reductions in clinical errors and duplicity due to inefficient data exchange between providers, and reduction in administrative costs generated by the efficiencies of EHRs over maintaining paper records.

When the total fraud- and non-fraud-related costs and benefits are combined, the net values will vary in magnitude depending upon the underlying IT infrastructure. By addressing both fraud- and non-fraud-related costs and benefits, a more comprehensive assessment of the actual value of the NHIN can be ascertained under each of the future IT scenarios.

CONCEPTUAL MODEL AND ASSUMPTIONS

The conceptual model for this analysis is straightforward. A consumer/potential patient derives a benefit from medical care through an improvement in their health status. Fraud activities diminish consumer welfare by either incurring additional cost—directly or indirectly—to patient care or the consumer's insurer.

Two types of fraud-related benefits can be articulated: IT enhancements that *detect* fraud and IT enhancements that *prevent* fraud from occurring. Investment in IT enhancements that result in prevention may never be recognized. Nevertheless, it is what economists consider an opportunity cost.

With respect to healthcare IT, economists place a value on the

benefit derived from the increased use of EHRs from two perspectives: opportunity cost and "foregone cost." For example, an opportunity cost derived from the use of EHRs would be the prevention of a medical error (valued as a non-fraud related benefit). In the case of investment in activities that result in fraud-related benefits, the investment in prevention foregoes the alternative of potential fraud creation.

The methods used in this analysis are common within the context of medical technology evaluation studies, where the costs and benefits of a new treatment are compared to that of a traditional therapy. As such, this method does not involve a formal economic model. Rather, it relies on economic principles of consumer welfare analysis and monetary valuation of the aforementioned opportunity costs following the approach outlined in the comprehensive review of the field by the Institutes of Medicine.[8] This approach requires an inventory of the estimated costs and benefits of different technologies scaled to the level of citizen and then multiplied by the size of the potential population affected. In this case, the scope of the NHIN is truly societal; all of our results are measured in 2005 dollars as expressed as national costs or benefits.

The playing field of fraudulent activity is constantly changing. Therefore, maintaining effective fraud management tools demands continuous re-assessment of emerging fraud trends and constant revision of controls.

The approach was designed with future enhancement and adaptation in mind. Many of the cost and benefit items used are generated either from assumptions derived from actual healthcare IT cost studies or expert opinion. As current and future research in healthcare IT valuation increases, cost and benefit items in this model can be revised and updated. In future enhancements to this model, where the trajectory of the NHIN scenarios are set to specific timetables with all stakeholders committing to firm milestones, this method can be used to develop a multi-year projection that describes the trajectory of costs and benefits. The approach used for this analysis assumes the annual costs of systems with annualized estimated transition costs amortized into the scenario by simply scaling any multi-year capital cost expenditure as an additional annual cost.[9]

FOUR STATES OF THE WORLD

The analysis assumes four states of the world for fraud- and non-fraud-related cost and benefit comparison. Each state is described as follows:

State 1: Status quo without interoperability. This is the present state of the world. For the most part, healthcare IT data systems are stand-alone systems owned by different stakeholders in the health economy and include paper-based medical records in provider practices. The principle health IT data generators in this world are medical providers[10] and public and private insurers. With the exception of integrated delivery systems, data reside in institution-specific silos except for payment and prescription transactions. This world is assumed to include early use of e-prescribing introduced in response to Medicare Part D. With regard to fraud, e-prescribing presents a new vulnerability because of the increased velocity of authenticated automated transactions.

State 2: Early EHR with no interoperability. This is a future state where elements of an EHR—such as diagnostic testing results and e-prescribing—become common transactions among providers, insurers and consumers. There is an increased use of EHRs, but interoperability does not exist.

State 3: Intermediate NHIN with interoperability and intelligent coding tools. In this state, the NHIN has been implemented with record-locator technology, enabling clinical data interchange among provider systems and payors. Additionally, intelligent coding tools are being used, providing improved context for the coding of treatments or diagnoses. For example, the NHIN is more likely to be using ICD-10 codes, which can document a person's true health disposition with greater precision and accuracy than ICD-9 codes. Though ICD-10 codes will not completely prevent fraud, more precise coding may deter "gray area" fraud, such as up-coding.[11]

State 4: Advanced NHIN with interoperability and analytic tools. This state builds on to the previous state of an assumed NHIN infrastructure with new analytic tools to detect fraud. These tools analyze treatment patterns by aggregating a patient's clinical data across providers and over time. They rely on algorithms that use record-locater technology to verify patient disposition and outcomes based on a scan of all available data prior to payment. Record-locator technology also can be used for random cyber audits; certain are referred for investigation to identify fraud activities. The advanced NHIN is a completely computerized system and possesses an element of predictability that can possibly be exploited. Effective fraud management requires an advanced dynamic element of investigation to match innovative cyber-criminals.[12]

COSTS AND BENEFITS INVENTORY

An inventory of the costs and benefits associated with each of the four states has been compiled. This inventory is based on a review of the healthcare IT literature and expert opinion available through the Economic Fraud Working Group and Executive Committee of the Department of HHS. Once a cost or benefit was identified, a monetary value was taken from either the clinical literature or expert opinion and scaled to a per US citizen value. A similar approach was used by Walker et al. to estimate the net benefit of an interoperable health IT infrastructure.[13]

IDENTIFYING THE COSTS

When an industry or organization implements a change, it does not happen without costs—even if the change streamlines and improves the product/service being delivered. When the proposed change does not have a direct impact on the actual product or service, a more careful analysis of the costs associated with implementation is warranted. Therefore, a breakdown of costs

associated with activities related to fraud detection, deterrence and recovery, and costs related to non-fraud activities, such as introducing a new IT system, is needed.

Because healthcare represents such a large portion of US spending, it will continue to provide fertile ground for criminals. Therefore, we believe that fraudulent behavior—and the costs associated with it—will remain a fixture even under the most interoperable IT platform. In addition, the costs associated with public and private industry investigation and prosecution will remain on the horizon. Finally, intelligence and analytic tools specifically designed and maintained to detect, deter and recover losses suffered as a result of fraud will be necessary for the system to be complete.

The costs related to implementing any type of IT system can be grouped into three basic categories: system/hardware changes, training costs and lost productivity costs. Based on the presumption that IT investment will occur across the entire healthcare industry (physician, hospital and other providers), we estimated and divided the cost of IT implementation into the following four types of investment among the different provider categories:

1. **Capital costs.** Capital costs represent a significant burden. However, the difference between the basic investment and the most advanced should provide an incentive to providers to consider interoperability a real value.
2. **Operating costs.** Operating costs include the cost of hiring, training and/or re-training staff.
3. **Interoperability transition costs.** Since many providers have already made the capital and operations investments in IT systems, they will have to achieve interoperability at some point in the future.
4. **Data storage costs.** Data storage costs will increase as interoperable capability is maximized.

Descriptions of the types of fraud-related and non-fraud related costs and benefits are as follows:

COSTS

Fraud-related: These costs represent the most direct burden of fraud expenses on the healthcare system. They include the actual costs of labor and materials to detect fraud and the interdiction of the fraudulent operation, as well as the actual monetary outlay that has been paid out. Many of the costs used are extrapolations from the CMS Office of Inspector General Semi-Annual Report (October 2003-March 2004) and other are opinions of the expert workgroup. The fraud-related costs include identity theft, which can be defined as the use of either a patient's or a physician's ID number in order to submit a claim; billing for services that were never completed using either a real or fictitious provider ID; providing unnecessary services solely for the purpose of revenue generation; up-coding and/or the misrepresentation of the complexity of treatment; Medicare and Medicaid annual expenditures on fraud detection and prosecution; private sector annual expenditures on fraud detection and prosecution; the costs of intelligent tools to martial data from the EHR; and the costs of development and maintenance of fraud detection analytic tools.

Non-fraud related: These costs primarily represent the investments necessary to implement the various IT infrastructures under the different scenarios. A recent article by Kaushal et al. (2005) provided much of the basis for the estimated annual and ongoing operating costs of a NHIN and other states of the world.[14] The non-fraud related costs include the capital investment costs for IT of physicians, hospitals and other healthcare providers (i.e., SNF, pharmacy, etc.); the annual operating costs to maintain and update IT systems of physicians, hospitals and other healthcare providers; and other costs, such as data storage costs for retention and transition costs for providers to scale up to higher levels of interoperability.

BENEFITS

Fraud-related: The fraud-related benefits of various IT platforms are associated with any recovery of fraudulent payments as well as the prevented or opportunity costs of fraud detection. These estimates are based on the OIG report (2004), the RAND analysis of ICD-9 to ICD-10 conversion and its net impact on fraud prevention, as well as expert opinion. The fraud-related benefits include the annual recovery of payments made by the government and private sector payors for fraudulent claims; the net benefit of gaining more accurate depictions of disease and reducing the likelihood of fraudulent up-coding; the identification of new leads from more digital fingerprints, as related to fraud; the verification and validation of actual services through phone call-back or web-based services; patient verification of services through the web or through an EHR portal; digital verification of services rendered by actual patients and providers; the reduction in record assembly time by use of common identifier and increasing digital media; the automated digital authentication to authorize claims billing and payment; the real-time verification of benefits eligibility and possibly debit payments in the case of HSAs; and the reduction in consumer time spent to deal with the consequences of fraudulent claims.

Non-fraud-related: The argument for the societal benefits of an improved health IT infrastructure have been documented by the studies citied in the Institute of Medicine's Cross the Quality Chasm (2001) report as well as the HHS Strategic Health IT Framework (2004). To develop a counter balance to the significant investment costs of developing an NHIN, the non-fraud related benefits are detailed. The sources for these estimates include the Walker et al. (2005) estimated savings from an NHIN,[15] studies documenting avoidable medical error where an NHIN may have an impact,[16] as well as expert opinion.

The non-fraud related benefits include avoiding the duplication of laboratory and imaging tests; avoiding the gathering of redundant information already available digitally elsewhere; less labor time needed to verify eligibility; less material and labor time needed to service paper documentation; less time needed to store and retrieve paper records; a reduction in the time needed for the consumer in phone trees and recording unnecessary information (i.e., reviewing EOBs); a reduction in societal medical costs and loss of life due to medication errors; a reduction in societal medical costs and loss of life due to clinical errors (i.e., operating on the wrong limb); a reduction in societal medical cost of unneeded diagnostic tests; a reduction in societal medical cost of unneeded medical surgeries; a reduction in malpractice costs and legal fees paid on

Table 1: Fraud-related annual costs.

Population: All US		States of the World (in millions)			
	295,743,134	1-Status	2-Hybrid	3-Intel	4-Analytic
Costs					
Fraud-Related					
Identity Theft for Any Purpose		$ 1,166	$ 1,400	$ 1,050	$ 700
Faked Services Under Fictitious Provic		$ 591	$ 9,463	$ 1,774	$ 237
Faked Services Under Real Provider II		$ 37	$ 48	$ 22	$ 7
Unnecessary services for revenue only		$ 25,878	$ 31,053	$ 10,351	$ 5,176
Upcoding & mis-representation of trea		$ 22,181	$ 26,617	$ 4,436	$ 2,218
Govt. Investigation & Prosecution		$ 286	$ 343	$ 372	$ 400
Non-commercial Investigation & Prose		$ 429	$ 515	$ 558	$ 601
Intelligent costs		$ -	$ 450	$ 900	$ 1,080
Analytic Tools		$ -	$ 540	$ 540	$ 2,700
SUBTOTAL		**$ (50,568)**	**$ (70,429)**	**$ (20,003)**	**$ (13,118)**

per case basis due to improvements in avoidable error; a reduction in additional physician costs associated with ER and avoided hospital services; a reduction in additional pharmacy costs associated with ER and avoided hospital services; a reduction in referral visits to screen future care provider through some screening from pay for performance (P4P) initiatives; and a reduction in provider time, bundling, storing, and forwarding of records to patients, other providers and health plans.

EXPECTED CHANGE IN BENEFITS AND COSTS UNDER DIFFERENT SCENARIOS

With an inventory of costs and benefits—both fraud-related and not—monetized for a societal annual impact, the estimated change was considered by expert opinion based on previous experience and expectations of the NHIN rollout. For example, there was a 100 percent change expected for the use of digital signatures to identify fraud under the status quo because it simply does not exist currently as a technology option. In the two NHIN states of the world, State 3 and State 4, the benefit associated is recognized, but only to the fullest extent with the use of analytic tools.

States 3 and 4 in the model are recognized as the most subjective. As a result, several working rules were used to make the estimates shown later in this section. First, whenever possible, empirical evidence was sought. When it was not available, a conservative estimate was used and then discussed as appropriate. A second rule was that the difference between States 3 and 4 assumes that the operations in State 4 are the most advanced because of prior experience gained reaching the state, including new and unforeseen uses of the data that do not just benefit fraud detection, but also improve clinical efficiency and productivity. A final rule was to minimize double-counting benefits that are closely related. As a result, more granularity than less was used to identify and quantify benefits to disentangle the overlap. If overlap proved unavoidable, expected changes were made more conservatively between the two correlated benefits.

RESULTS

Table 1 presents data indicating that the healthcare industry is vulnerable to fraud and perpetrators of fraud will continue to attempt to outwit the system regardless of the fraud management and detection tools being used. The dramatic fraud-related costs in the Status Quo and Early EHR states are the inevitable result of the increasing predictability of electronic claims processing[17] coupled with the lack of the intelligent and analytic components of State 3 and State 4[18] that would make claims submitted and paid electronically safer.[19] States 1 and 2 both assume the increased costs of fraud related to the new Medicare Part D prescription drug benefit.

Table 2 captures the costs associated with the initial capital investments and the ongoing operating costs that healthcare providers must make in order to implement IT systems that increase in their intelligence and analytic capabilities. In addition to large up-front investment, cost-savings are only realized in the medium to the long term.[20] The issue is not whether to implement the use of IT to detect fraud, rather how to equip fraud management teams with the best technological tools possible,[21] and given the dynamic nature of fraud, investment in new detection tools to ferret it out is always needed. Funding has also proven to be the main barrier to the adoption of EHRs.[22]

Note that capital investment costs are considerably higher than operating costs. This model assumes that increasing interoperability will create greater standardization of data elements and modularization of the features in provider's EHR application and will lead to lowered or neutral changes in operating expenditures. In addition, costs for providers learning new systems are reflected in interoperability transition costs.

Table 2: Non-fraud related annual costs.

Population: All US	295,743,134	States of the World (in millions) 1-Status	2-Hybrid	3-Intel	4-Analytic
Non-Fraud Related					
Capital Investment					
Physicians		$ 880	$ 968	$ 1,012	$ 1,056
Hospitals		$ 2,780	$ 3,058	$ 3,197	$ 3,336
Other Providers		$ 1,080	$ 1,188	$ 1,242	$ 1,296
Operating Costs					
Physicians		$ 240	$ 264	$ 276	$ 288
Hospitals		$ 720	$ 792	$ 828	$ 864
Other Providers		$ 380	$ 418	$ 437	$ 456
Data Storage		$ 1,461	$ 5,843	$ 11,686	$ 14,607
Interoperability transition costs					
Physicians		$ -	$ 4,355	$ 12,194	$ 13,936
Hospitals		$ -	$ 11,980	$ 33,544	$ 38,336
Other Providers		$ -	$ 8,130	$ 22,764	$ 26,016
SUBTOTAL		**$ (7,541)**	**$ (36,996)**	**$ (87,180)**	**$ (100,191)**

Table 3 reflects the reality faced by the healthcare industry: that emerging patterns of fraud seem to pass unnoticed until enormous amounts of damage are done.[23] Therefore, in the world of State 1, benefits are primarily derived from the recovery of funds after fraud has been committed.[24] The benefits that are projected with the introduction of electronic health records coupled with e-prescribing in State 2 offer only a glimpse of the benefits that intelligent (State 3) and analytic (State 4) tools could offer in an interoperable environment.[25]

Table 4 quantifies the substantial benefits that can be captured that are non-fraud-related. In a State 4 interoperable world, the clinical and administrative benefits that would result from providers (hospitals and medical group practices) and independent laboratories, radiology centers, pharmacies, payors and public health departments being able to exchange electronic data would be substantial.

Table 5 combines the costs and benefits quantified in Tables 1 through 4 and provides the net values that can be expected based on the assumptions for each scenario. The modest increase in fraud related benefits of the early NHIN is offset by the increase

Table 3: Fraud-related annual benefits.

Population: All US	295,743,134	States of the World (in milli 1-Status	2-Hybrid	3-Intel
Benefits				
Fraud-Related				
Government Recovery		$ 1,144	$ 1,258	$ 2,860
Private Sector Recovery		$ 458	$ 504	$ 687
Conversion to ICD10		$ -	$ -	$ 90
Digital tracing for Fraud		$ -	$ 53	$ 111
Patient verification of Dx & Procedure		$ -	$ 89	$ 185
Provider Verification of Dx		$ -	$ 1,800	$ 5,700
Digital certificates & signatures		$ -	$ 786	$ 1,638
Reduction in record retrieval time		$ -	$ 2,359	$ 5,504
Authentication		$ -	$ 393	$ 819
IDs only from card swipes		$ -	$ 393	$ 819
Avoided time spent for fraudulent claims		$ 131	$ 786	$ 2,621
SUBTOTAL		**$ 1,733**	**$ 8,422**	**$ 21,033**

Table 4: Non-fraud related annual benefits.

Population: All US	States of the World (in millions)			
295,743,134	1-Status	2-Hybrid	3-Intel	4-Analytic
Benefits				
Non-Fraud Related				
Real time patient data for ER situations	$ 1,271	$ 7,626	$ 12,710	$ 15,887
Less time tracking identity for $$ eligibili	$ 786	$ 4,717	$ 7,862	$ 9,828
Less use of paper	$ 322	$ 1,932	$ 3,221	$ 4,026
Less staff to manage paper	$ 1,048	$ 6,290	$ 10,483	$ 13,104
Less consumer time integrating benefit i	$ 89	$ 532	$ 887	$ 1,109
Avoided Medication Errors	$ 254	$ 1,525	$ 2,542	$ 3,177
Avoided Clinical Errors	$ 444	$ 2,662	$ 4,436	$ 5,545
Avoided Duplicate Diagnoses	$ 2,597	$ 15,582	$ 25,969	$ 32,462
Avoided Unnecessary Surgeries	$ 844	$ 5,065	$ 8,442	$ 10,552
Avoided Liability for Medical Error	$ 36	$ 288	$ 432	$ 540
Less physician $$ due to avoided error/	$ 3,382	$ 20,294	$ 40,588	$ 50,735
Less pharmacy $$ due to avoided error/	$ 1,691	$ 10,147	$ 20,294	$ 25,368
Less time provider shopping	$ 177	$ 1,065	$ 1,774	$ 2,218
Less consumer time managing med rec	$ 89	$ 532	$ 887	$ 1,109
SUBTOTAL	**$ 13,031**	**$ 78,258**	**$ 140,528**	**$ 175,660**

in fraud related costs, making this a wash from the fraud management standpoint. It is not until States 3 and 4 that fraud management becomes truly net positive. This change occurs because interoperability has tremendous potential to lower fraud-related costs. Interoperability allows for corroborating the validity of online and automated transactions from multiple data sources for any given patient in real or near real time.

Since efforts to introduce and encourage adoption of electronic health records have been only mildly successful, it is tempting to advocate attempting to skip over State 2 altogether.[26] Interoperability and a demand for cross-entity standardization of codes, data structures and terminologies may be the key to create the necessary incentive that will facilitate adoption and minimize the transition costs while preserving the benefits.[27]

DISCUSSION

Three major findings were identified from this analysis. First, substantial savings can be expected from fraud-related expenditures that can be realized from a move to an interoperable NHIN that are not realized in the status quo or early non-interoperable NHIN.

Second, the most dramatic improvement in fraud net cost/benefit may be achieved in moving to the State 3 NHIN with interoperability and intelligent tools. The early NHIN state is nearly as costly as the status quo in terms of the net fraud-related costs and their impact on the US health economy. Some of the assumed extra cost in both the status quo and early NHIN states come from the new fraud opportunities created by Medicare Part D.[28] Similar findings were reported in the Spring 2003 RAND Corp. study of the costs and benefits associated with transitioning from ICD-9 codes to ICD-10. They found that the lack of coordination and unfamiliarity with a new system would lead to a greater error rate, and until training is complete there would be an increase in cost.

Libicki and Brahmakulam suggest that a new coding system, such as ICD-10, would present an increased opportunity for fraud in the beginning because people are less familiar with the new codes. It might be more difficult to detect potential duplicates, unbundled services or up-coding during a transition period when two code sets would be in effect. Long term, however, it is possible that fraud could be reduced since ICD-10-CM and ICD-10-PCS are more specific and there are fewer "gray" areas in coding.[29] And, once the transition is complete, the use of the ICD-10 codes would result in an estimated $100 million to $1 billion fewer fraudulent claims being paid.[30] These studies highlight the fact that any transition designed to enhance and expand IT capabilities creates a distraction that allows the predictability factor to encourage fraud. Finally, the non-fraud related benefits associate with the intelligent and analytic tools in States 3 and 4 are substantially higher than the fraud related benefits, leading to the realization that interoperability pays for itself.

Results from this analysis should be interpreted with caution. The estimates presented are based on an economic impact model populated by the results of empirical studies on the costs of fraud prevention and health IT transition costs. However, many elements required expert estimation. At the very least, this analysis provides a structure for new evidence to be added so that areas where only expert opinion was available can be replaced with new empirical findings.

It is also important to recognize that the aggregate economic analysis undertaken here does not consider the actual distribution of the costs and benefits among the individual stakeholders

Table 5: Summary of annualized costs & benefits.

Population: All US	295,743,134	States of the World (in millior 1-Status	2-Hybrid	3-Intel
Costs				
Fraud-Related				
SUBTOTAL		$ (50,568)	$ (70,429)	$ (20,003)
Non-Fraud Related				
SUBTOTAL		$ (7,541)	$ (36,996)	$ (87,180)
Total		$ (58,108)	$ (107,425)	$ (107,183)
Benefits				
Fraud-Related				
SUBTOTAL		$ 1,733	$ 8,422	$ 21,033
Non-Fraud Related				
SUBTOTAL		$ 13,031	$ 78,258	$ 140,528
Total		$ 14,764	$ 86,679	$ 161,561
Net Cost (-) Benefit (+) - Fraud Only		$ (48,835)	$ (62,008)	$ 1,030
% Healthcare GDP		-3%	-4%	0%
Net Cost (-) Benefit (+) - Fraud and Non-Fraud		$ (43,344)	$ (20,746)	$ 54,379
% Healthcare GDP		-3%	-1%	3%

involved. Costs and benefits will not necessarily be distributed evenly or uniformly among all of the stakeholders.

The finding that interoperability could pay for itself—without consideration of fraud and abuse prevention—is not new. Walker, et al. found a similar result. This analysis concurs with Walker's finding using methods that are similar but not identical. In addition, the finding of a fraud-related net benefit further supports the value proposition of interoperability proposed by the NHIN.[31]

This analysis could be advanced by a continued exploration to detail the trajectory and timing of the different states of the world. Such an analysis would produce a more advanced set of findings that would describe five-, 10- and even 15-year net benefit calculations. This type of analysis would be particularly helpful to ascertain the optimal length of time for a transitory state, specifically for the early EHR. In addition, a future long-run analysis might also benefit significantly from an NHIN that results from a combination of unmeasured network externalities. Of course, a long-time horizon with a more complex digital infrastructure may not affect fraud prevention without continuing efforts and stewardship to thwart any new possible fraud schemes.

SUMMARY AND RECOMMENDATIONS

Two recommendations emerge from using an economic framework to look at the possibility of healthcare fraud management through the expansion and enhancement of IT that merit further discussion and investigation. First, given that the early NHIN state of the healthcare IT world is associated with relatively high costs compared to the benefits derived, it seems prudent to limit exposure to this state as much as possible. Consider limiting exposure to the early EHR state to no more than two years. Given that this state of the world is associated with high expense, it seems prudent to visit this state for as little time as possible. It is an understandable transition point and most likely a necessary one, but it should be clear that it is nothing more than a transition point. Second, move to an NHIN with advanced analytic tools as quickly as possible. Although interoperability by itself provides the most dramatic net fraud-related cost/benefit improvement, the addition of advanced analytics provides a substantial improvement in both fraud and non-fraud related benefits.

CONCLUSIONS

Healthcare fraud is a major problem in the US healthcare system. It impacts patient safety and providers' abilities to deliver quality care at an affordable cost. Escalating premium costs and the associated implications contribute to the need for deliberate deployment of the NHIN with interoperable EHRs. The need for portable health information has never been more evident than it was in the aftermath of Hurricane Katrina, in 2005. Many paper-based health records were destroyed or badly damaged. An NHIN designed with fraud management requirements and interoperable capabilities would provide a level of protection against losses that might result from a man-made or natural disasters, as well as fraud schemes.

Healthcare fraud hurts all stakeholders. The full extent of healthcare fraud is unknown as there are no systematic measurements for fraud statistics, monitoring or reporting. Fraud is dynamic and constantly evolving. As such, it requires ongoing active surveillance using information technology and aggressive consumer involvement. Vigorous prosecution of healthcare fraud can be a powerful deterrent, but stopping fraud before it happens is an even more effective cost-saving measure.

It is essential that fraud management programs be built into the NHIN infrastructure as part of its early design. Designing fraud management functionality into the NHIN has the potential to significantly reduce healthcare fraud losses. The interoperability between multiple EHRs is a major enabler of these loss reductions. Maximum benefit will be achieved by linking a claim with its corresponding documentation from an EHR, this will provide the ability to access information in other provider's EHRs regarding the same patient, and to apply advanced analytics to aggregate clinical and financial databases. Without a deliberate effort to build fraud management into the NHIN, healthcare payors and consumers will be exposed to new and potentially increased vulnerability to electronically enabled healthcare fraud.

The conventional thinking is that the adoption of EHRs and participation in an interoperable NHIN will not be mandated, but voluntary. While there are certainly many understandable reasons for such an assumption, it is apparent that the most aggressive perpetrators of fraud will almost certainly opt out of the NHIN to avoid its anti-fraud capabilities. Thus, the architects of the NHIN, and those involved with payment systems, may want to consider the advantages and disadvantages of a system that at some point in the future might predicate payment of claims on participation in the NHIN, assuming of course that this becomes technologically and economically feasible. While such linkage would certainly increase the anti-fraud potential of the NHIN, strong consideration must be given to the fact that this might seem unduly coercive and could mandate significant added costs for certain providers.

National metrics for fraud management are required to systematically gauge and reduce healthcare fraud. Public and private stakeholder collaboration, as well as interstate cooperation, is also required to fight healthcare fraud. Such an anti-fraud enabled NHIN has the potential to identify emerging fraud schemes prior to payment. A shift from the current "pay and chase" fraud management programs to the proactive prevention of fraudulent claims prior to payment is made possible by interoperable EHRs and advanced analytics.

In conclusion, substantial savings in fraud-related expenditures would be enabled by an NHIN. It is important, however, to move quickly through the early transition state of the NHIN and achieve widespread adoption in order to maximize net savings. **JHIM**

ACKNOWLEDGEMENTS

This project was supported by The Office of the National Coordinator for Health Information Technology, HHS. Contract Number: HHSP23320054100EC.

Stephen T. Parente, PhD, is Assistant Professor in the Department of Finance at the Carlson School of Management, University of Minnesota, Minneapolis.

Karen Mandelbaum, JD, is an attorney at the firm of Tilton & Dunn, PLLP, in St. Paul, Minn.

Susan P. Hanson, MBA, RHIA, FAHIMA, is President of TerraStar Consulting Services.

Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS, is President of Cassidy & Associates.

Donald W. Simborg, MD, is the co-founder of HL7 and founding member of AMIA's College of Medical Informatics.

REFERENCES

1. Martin S. Advanced card-fraud-detection system and SAS building. *Information Week*. July 21, 2005.

2. Centers for Medicare & Medicaid Services. Available at: http://www.cms.hhs.gov/.

3. Pressler MW. Signs of fraud go beyond signature: Credit card companies use artificial intelligence to thwart thieves. *Washington Post*. July 21, 2002; (H05).

4. US Department of Health and Human Services. The decade of health information technology: Delivering consumer-centric and information-rich health care. July 2004.

5. Darby MR, Karni E. Free competition and the optimal amount of fraud. *J Law Econ*; 16(1):67-88.

6. National Health Care Anti-Fraud Association. Healthcare fraud: A serious and costly reality for all Americans. Available at: http://www.nhcaa.org/eweb/StartPage.aspx. Accessed August 14, 2005.

7. Sparrow MK. *License to steal: Why fraud plagues America's health care system*. Westview Press. Boulder, Colorado. 1996.

8. Gold MR. *Cost-effectiveness in health and medicine*. Oxford University Pres: New York, New York, 1996.

9. As a starting point for this analysis, no discount factors are used because the growth and scale of the expenditures for an NHIN remains unknown is likely to be non-linear. Thus, assuming a linear discount factor, for example, might produce results due more to speculative discounting than actual technology cost differences.

10. Medical providers are defined generally as physicians, hospitals, pharmacists and other person or institution engaged in the delivery of heath services.

11. Libicki M, Brahmakulam I. The costs and benefits of moving to the ICD-10 code sets. The RAND Corporation Science and Technology Institute. March 2004.

12. Sparrow MK. *License to steal: Why fraud plagues America's health care system*. Westview Press. Boulder, Colorado. 1996.

13. Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Blackford M. The value of health care information exchange and interoperability. *Health Aff*. January 2005.

14. Kaushal R, Blumenthal D, Poon E, Jha A, Franz C, Middleton B, Glaser J, Kuperman G, Christino M, Fernandopulle R, Newhouse J, Bates DW. The costs of a national health information network. *Ann Int Med*. 143(3):165-173.

15. Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Blackford M. The value of health care information exchange and interoperability. *Health Aff*. January 2005.

16. Zhan C, Miller M. Excess length of stay, charges and mortality attributable to medical injuries during hospitalization. *JAMA*. 290(14):1868-1874.

17. Sparrow MK. *License to steal: Why fraud plagues America's health care system*. Westview Press. Boulder, Colorado. 1996.

18. Fair Isaac.com. Available at http://www.fairisaac.com/fic/en/. Accessed July 28, 2006.

19. Id. at 137.

20. Brailer DJ, Terasawa EL. Use and adoption of computer-based patient records. California HealthCare Foundation. October 2003.

21. Sparrow, M.K., License to Steal: Why Fraud Plagues America's Health Care System, Westview Press, Boulder, Colorado, 1996.

22. Baron RJ. Electronic health records: Just around the corner, or over the cliff? *Ann Int Med.* 143(3):222-226.

23. Id. at p. 38.

24. Schneider A. Reducing Medicaid fraud: the potential of the false claims act. Available at: http://www.taf.org/publications/PDF/drug%20report.pdf.

25. Libicki M, Brahmakulam I. The costs and benefits of moving to the ICD-10 code sets. The RAND Corporation Science and Technology Institute. March 2004.

26. Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Blackford M. The value of health care information exchange and interoperability. *Health Aff.* January 2005.

27. Brailer DJ, Terasawa EL. Use and adoption of computer-based patient records. California HealthCare Foundation. October 2003.

28. RX for fraud: scamsters can't wait for Medicare's new $720 billion pill plan. *Forbes.* June 20, 2005.

29. Libicki M, Brahmakulam I. The costs and benefits of moving to the ICD-10 code sets. The RAND Corporation Science and Technology Institute. March 2004.

30. *Ibid.*

31. Walker J, Pan E, Johnston D, Adler-Milstein J, Bates DW, Blackford M. The value of health care information exchange and interoperability. *Health Aff.* January 2005.