BEYOND

REPEAL AND REPLACE

IDEAS FOR REAL HEALTH REFORM

Harnessing Health Information in Real Time: Back to the Future for a More Practical and Effective Infrastructure

Stephen T. Parente

A PROJECT OF THE AMERICAN ENTERPRISE INSTITUTE

BEYOND REPEAL AND REPLACE

Harnessing Health Information in Real Time: Back to the Future for a More Practical and Effective Infrastructure

By Stephen T. Parente

A PROJECT OF THE AMERICAN ENTERPRISE INSTITUTE
DECEMBER 2010

Editor's Note

The long-sought goal of widespread use of health information technology (IT) and electronic health records to improve the performance of U.S. health care has faced stubborn barriers to implementation over the past decade. Last year, the Obama administration and Congress chose to pursue another climb up the steep hill of health IT development. The American Recovery and Reinvestment Act of 2009 injected unprecedented amounts of funding, along with new financial incentives and disincentives, to achieve broader adoption of interoperable health IT systems.

As part of the AEI project Beyond "Repeal and Replace": Ideas for Real Health Reform, health industry analyst Stephen T. Parente questions whether this strategy is likely to overcome longstanding economic disincentives to the use of electronic health records, particularly in physicians' private practices. He suggests that policymakers instead should draw upon the lessons of the financial services industry's experience in implementing IT several decades ago. Parente recommends an approach that uses integrated-health-card technology to build on the current transaction-based system for health insurance. He proposes that expedited payment incentives could enrich it with additional data of high clinical value.

Parente offers a clear, market-oriented alternative to the current centralized health-IT procurement approach, which is supplemented with insufficient bribes and penalties to achieve private-sector compliance with interoperability standards. He concludes that this more practical "back to the future" path to harnessing health information in real time can deliver long-overdue dividends in medical-fraud control, insurance-coverage administration and underwriting, and improved health care quality.

Stephen T. Parente *is a professor of finance and insurance at the University of Minnesota and the director of the Medical Industry Leadership Institute.*

Harnessing Health Information in Real Time: Back to the Future for a More Practical and Effective Infrastructure

Health information technology (IT) is a critical component of a high-performance health care industry. At its best, this technology can not only alert a patient or physician to past medical history to avoid redundant services and diagnostic tests, but also provide new information to save someone's life and offer previously unknown options for health improvement and medical care financing. As a result, calls to action for widespread adoption of electronic health records have come from a broad spectrum of private organizations and public policymakers.

The problem is that the calls to action are getting stale, after nearly two decades of national declarations beginning during the presidency of George H. W. Bush in the early 1990s. Today the Obama administration has committed itself to widespread use of electronic health records and supported the American Recovery and Reinvestment Act of 2009 (ARRA), which earmarks an unprecedented amount of $34 billion for health IT. This study contends that, while commendable in intent, the current pathway being executed by the Obama administration for creating interoperable medical records will most likely fail to achieve its ambitious vision by 2015. It compares that approach with a U.S. technology deployment effort of comparable magnitude, namely the real-time financial services transaction system and how it relied on identifying and aligning incentives in the private sector rather than using government subsidy and architecture to achieve its ambitious vision. The study concludes with both a vision and a tactical plan for how health IT initiatives currently underway can be adapted so that health IT finally achieves the aims identified by the last four U.S. presidential administrations.

The Opportunity at Stake

There is broad agreement that robust health IT can lead to less costly and more productive medical care. The problem is that only a few people understand what needs to be done tactically at the ground level to achieve this high-level goal. One way to imagine what the opportunity at stake could be is to consider, as a comparison, China's health IT efforts. On a national scale, China has debuted an electronic health-records system. Unhindered by the legacy IT platforms developed in the United States over the last three decades (for example, mainframes, minicomputers, and unnetworked IBM-clone microcomputers), China is simply building a single Internet-based electronic health-records system that all providers will use. The system was designed three years ago and became available in 2009. This development

would be the U.S. equivalent of Medicare requiring that all physician payments route through a contract awarded to Paypal.com. Now imagine if the Chinese medical-records system becomes ubiquitous for all providers by 2012, three years ahead of the ARRA-funded initiatives. It would enable medical-research keyword searches for clinical-trial analysis and reporting at a scale never imagined in any U.S. medical institution—creating a supply chain for a medical care health IT platform that resembles FedEx package tracking more than highly fragmented hospital-specific IT installations.

But instead of building one standardized, Internet-based, quick-to-deploy, real-time electronic health-records systems, the United States has embarked on a much slower development path by funding competing health IT vendors that may never integrate data together, for the benefit of the patient, in real time. The ARRA seeks to create linkages of data not by the command-and-control infrastructure policies most similar to China, but by interoperable data vendors.

In today's U.S. health care system, the proponents of interoperability-bridging institutions for health IT have failed to draw upon the experience of the financial services industry several decades ago. That sector learned there was more to gain by limited cooperation and data exchange, to prevent billions of dollars in credit card fraud. The same lessons apply to the health care IT industry today, in terms of opportunities ahead for health care IT investments and applications ranging from fraud mitigation to comparative effectiveness research.

We should embrace and innovate from what is a core asset: transaction-based, fee-for-service health insurance data. If this transaction-based system had more clinically relevant and health-outcomes data, it would provide a more effective substitute for an ARRA-financed health IT platform, and it could become a full-fledged electronic medical record. If the patient could also add information to the record, perhaps even on a transaction-specific basis (for example, about a lab test, prescription order, or physician visit), the result would be a very powerful technology because it would provide information on health care outcomes as well as expenditures. This would create the data needed for pay-for-performance as well as value-based insurance design and would be a necessary (but not sufficient) condition to transform the U.S. health care delivery system.

The Origin of Publicly Financed Health IT

The call for widespread adoption of electronic medical records as a cure for health care system inefficiency and waste is becoming an old saw. The effort got a kick start from the Institute of Medicine's companion monographs *To Err Is Human* (1999) and *Crossing the Quality Chasm* (2001). The authors of those books were most successful at identifying the value of health IT adoption as an opportunity cost. Specifically, they argued that without health IT investment, approximately 98,000 deadly medical errors per year would continue. Although the number reported was never verified by autopsy reports claiming "deficiency in health IT interface" as the reason for death,[1] the reports were a key motivator for President George W. Bush's push for health IT initiatives, and for the watershed moment in July 2004 when the Bush administration publicly assembled the largest delegation of federal and public-sector leaders ever to consider how to address the problem.

That 2004 meeting was memorable for two reasons. First, it formally introduced the concept of interoperable medical records as a goal, and it announced the first head of the Office of the National Coordinator for Health IT (ONCHIT), David Brailer, M.D.[2] Dr. Brailer developed and advocated the concept of interoperable medical records as part of his work in the late 1990s. At that time, Dr. Brailer was the chairman of Care-Science Inc., a health IT firm and provider of care-management services and Internet-based solutions.[3] One of the prototypes for interoperability was a community-based health information exchange he designed in Santa Barbara County, California.[4] Interoperability aimed to connect different providers' medical-records systems, if there was a common health IT standard, through a

health information exchange such as the one built in California.

The second memorable moment from the 2004 health IT summit was an exchange between health IT software vendors, when vendor 1 (of five on a panel) claimed that he was so impressed by the events of the day that he would make publicly available his proprietary source code for his firm's electronic medical record because he believed not linking records would lead to further unnecessary deaths. Vendor 3 also stated he was impressed with the events of the day, but seemed to joke that he was not impressed enough to give up his source code. To date, Vendor 3's candor has prevailed; the intellectual property that fuels the return on investment in the health IT industry is still dominant.

The problem with interoperability during the Bush administration was that it relied almost exclusively on health care providers' "virtue" regarding their willingness to invest in an electronic medical-records system, as well as share data in a data exchange. The Obama administration seems to have decided that virtue is not enough and proceeded with a strategy to bribe medical providers to buy an electronic medical-records system capable of linking to some health data exchange, and to tax them if they do not. The bribe comes from paying physicians ARRA funds to purchase an electronic medical-records system by 2014. The tax is the consequence of lower Medicare reimbursement for providers who have not purchased an interoperable electronic medical-records system by 2014.

The specific incentives were embedded in the meaningful-use requirements associated with the ARRA legislation. For example, the "meaningful use of EHR" is defined as the successful recording in 2011 of data such as the percentage of hypertensive patients with blood pressure under control. If these (and other) conditions are met by 2015, the Centers for Medicare and Medicaid Services (CMS) will not seek a penalty from noncomplying providers. Otherwise providers will pay a penalty going forward. An interim incentive in 2012 and beyond is cash inducement from ARRA to purchase sufficient health IT systems to meet the 2015 deadline. In effect, the Obama administration has more than doubled down on the Brailer's vision of interoperable IT with the ARRA health IT investment, on top of a weak carrot-and-stick proposal for mandated use of health IT systems.

One of the reasons the Obama administration upped the ante was that it expected much of the cost savings from health reform to come from advanced placement of new health IT systems. Harvard economics professor David Cutler, senior adviser to the Obama campaign and later an outside adviser to the administration, continued to make this assertion well after the 2008 presidential campaign ended.[5]

Lessons from Current IT Systems

In a parallel universe, throughout the United States there exists a national electronic medical-records system operating in near–real time and fully integrated with medical care practice. This universe is otherwise known as the U.S. Department of Veterans Affairs (VA). The VA runs the nation's largest network of government-owned hospitals and has one of the most extensive command-and-control medical care delivery systems in the world. The country is divided into over two dozen regions, each with a recognized VA central hospital and an affiliated academic medical center. Emanating from each of the regional centers is a network of community-based outreach centers that provide medical care and act as pharmaceutical dispensaries. The entire system is connected by a unified electronic medical-records system.

In comparison to private-sector medical care, the VA is a model of health IT deployment that leaves physicians who practice in both sectors wondering why their hospitals cannot be as modern as the VA. The answer is simply organizational incentives. Over two decades ago, the VA committed to a national health IT platform and had the authority to mandate the design of the system. The VA chose a vendor to build it and deployed it in the same way that a large national bank would roll out a new ATM interface system overnight. In short, if rapid and uniform IT deployment is your goal, command and control is a

formidable design. But it is completely inconsistent with the way private medical practitioners and hospitals organize themselves in the United States and with the incentives in place. By examining those incentives, we can understand what will make the Obama administration's ARRA-based health IT funding deliver subpar performance.

Other than official deadlines when providers will be penalized for not having purchased the right health IT solution, little transparent and measureable progress is being made.

Even relatively top-down private organizations that have been investing in health IT for decades—completely integrated managed-care organizations like Kaiser Permanente, large multispecialty group practices such as the Mayo Clinic, and large multihospital systems such as Hospital Corporation of America—lack the incentives to make their IT systems converse with each other. In addition to using different national health IT vendors for their primary electronic medical-records systems, the ability of the systems to converse with one another is an added feature for which each would have to pay both the electronic medical-records vendor and a consulting company such as Deloitte, Accenture, or Ingenix to "wire" in for them.

The ONC has gained some buy-in thus far on the pseudostandard of Health Level 7 (HL7) for systems to rally behind. However, HL7 was already well known; it was designed by IBM Consulting for system migrations from the 1990s forward. Furthermore, HL7 functions mostly as a forensic mapping document of features across systems. It does not facilitate a real-time data standard like that used by ATMs, so different vendors' electronic medical-records products can plug in to exchange data securely.

From the perspective of a patient in urgent need of medical care from multiple medical providers, the lack of integration can be quite frustrating. Without integration, tests are often repeated and time is wasted for both providers and patients. While waiting for the third identical blood test on the same day by three different doctors, a patient has to wonder whether providers are just scamming him or his insurer for more billings or, worse, whether it really is the case that providers refuse to link their systems even though such refusal can lead to more patient discomfort, clinical error, and longer waits.

Another disincentive to interoperability involves the legal counsel of a hospital or group practice. Legal counsel might suggest that revealing information about the care received at their facility by connecting to the health interoperability exchange would allow an outside physician or hospital to review the performance of the affiliated hospital's patient care. The reasoning continues that such an exchange would provide an easy hunting ground for data supporting medical malpractice suits. A hospital might conclude that the opportunity cost of avoiding medical malpractice is much higher than the economic value of a happy patient on his way to better health, after receiving faster and more appropriate care, due to the assistance of a completely interoperable medical record. The "do no harm" portion of the Hippocratic Oath might be interpreted as being as important an axiom for the health of the patient as for the financial health of medical practice.

Whether this is an actionable concern or not, practice leaders will likely see the threat of free-ranging patient data in an interoperable system as more of a cost to providing medical care than a savings. Thus, if the ARRA bribe and tax do not convey sufficient value, the Obama administration initiative will not work. Consider if five hundred thousand physicians all got a voucher to disperse the $34 billion health IT funds in the ARRA. That would amount to $68,000 per physician. Current medical malpractice insurance premiums run as low as several thousand dollars to over $100,000, depending on specialty and location. In 2002, for example, a large insurer in Minnesota charged base premium rates of $3,803 for the specialty of internal medicine, $10,142 for general surgery, and $17,431 for obstetrics-gynecology. In contrast, a large insurer in

Florida charged base premium rates of $56,153 for internal medicine, $174,268 for general surgery, and $201,376 for obstetrics-gynecology in Dade County, and $34,556, $107,242, and $123,924, respectively, for these same specialties in Palm Beach County.[6] Thus, a $68,000 value health IT voucher (the maximum value) may not be able to offset even one year of medical malpractice premium expense. With a payoff scenario like this, it may also be better to take a lesser Medicare reimbursement and avoid having to worry about the meaningful-use requirements of health IT systems.

To date, the progress of ARRA-funded health IT has been difficult to assess. Ideally, a progression of dollars would be spent by each quarter of the fiscal year and objectives achieved similar to any construction project. Instead, a visit to the ONC website reveals an expanding list of strategic initiatives that expand the mission without ever explaining how completion of a set of policy conferences yields a real-time health IT infrastructure. It appears that all possible topics that could be expanded upon, such as a set of conferences exploring uses of personal health records, are being pursued simultaneously with similar private-sector activities. In fact, most health IT development was private-sector driven before the ARRA funds and will likely remain so after dollars are exhausted. Other than official deadlines when providers will be penalized for not having purchased the right health IT solution, little transparent and measureable progress is being made.

In summary, the Obama administration's health IT advancement strategy is not novel, nor is it likely to change the economic disincentives for widespread adoption of electronic medical records in physician practices. We cannot rely solely on virtuous behavior by health care providers to ensure sufficient buy-in (both figurative and literal) to purchase interoperable health IT software and put it into operation. Moreover, the threat of using the data in malpractice cases—plus the vendor and the consulting cost of integration—may continue to discourage hopes that the current path for health IT implementation will lead to better systems or better patient care.

Looking to the Financial Services Industry for a Model for Real-Time Health IT

Interoperability has been successfully deployed in some industries, the most successful of which is the financial services industry. One of the largest differences between the medical community and the financial services industry is that the latter is largely rewarded for the velocity of information since it provides revenue with each transaction. To provide some perspective, the case of the financial services industry rallying against the threat from credit card fraud is considered below. To succeed, firms had to break from their "silo mentality" for storing and using data and agree to link their data for the collective purpose of avoiding fraud.

In the late 1980s, financial services firms were at a crossroads in identifying and preventing fraud. Tools and technology were immature, and firms used a "pay and chase" rules-based judgmental approach to "follow" fraud schemes. Culturally, key stakeholders were inclined to look at their solutions with a retrospective approach and only within their own credit portfolio. Fraud mitigation was a manual process based on a small number of fraud cases detected from prior experience. This process was highly ad hoc, retrospective, and put in place by hard coding cases into a credit card issuer's processing system. The rules did not adjust for new types of fraud schemes. It was typical that an issuer would have hundreds, and, in some cases, thousands of lines of code as they continued to implement new processes over time. At that time, fraud analysts "worked" transactions by reviewing computer printouts on their desks. This methodology did not allow firms to stop fraud effectively or efficiently before it occurred.

Furthermore, the detection methods at the time could not measure how much fraud was prevented or if a new test strategy or treatment was more or less effective than the previous strategy. It was easy for perpetrators to go undetected. If a perpetrator was identified, it was usually after numerous fraudulent transactions. Perpetrators often discarded stolen credit cards and moved their scheme to another issuer. Additionally, there was no process to

determine if the merchant was party to the fraud or colluding with a fraudulent credit card holder. Similar to medical providers or insurers, banks acting as credit card issuers did not share information; they operated within the silo of their own business and within their own market.

Many fraud transactions were inaccurately charged off as credit losses because issuers were unable to identify them as fraud or the account holders could not be located. Sometimes legitimate consumers paid for the fraud because they did not carefully check their monthly statements, which would have revealed charges made by fraud perpetrators. This hid the true scope of fraud in the industry and further perpetuated fraud losses. To move forward, the industry required a change of culture and practice supported by new technology that bridged data silos with highly structured and proprietary data systems.

In 1993, a technology-based incentive to change fraud detection in financial services arose: the introduction of predictive models for identifying fraud. Predictive modeling had historically been used in the financial services industry for underwriting credit and loans, and it was an accepted and proven method within the industry from several decades prior. The introduction of predictive modeling to prevent fraud was an extension and an enhancement of that methodology. The predictive-modeling technology is analogous in the U.S. health insurance industry to risk adjustment of medical claims data to determine future premiums or provider reimbursement.

Using predictive modeling to detect fraud was not a simple task. Similar to health care, the financial services industry had legacy mainframe and minicomputer technology as the core business processing system. Integrating a transaction-based fraud-detection system into the core business with strict time-processing standards was just one of many obstacles. This issue was eventually overcome by the fact that the savings from preventing fraud losses were many times greater than the investment to integrate and run the fraud-scoring systems.

A critical innovation was the development of a real-time fraud-scoring predictive model designed to perform real-time assessments on every single transaction. The volume of transactions handled was of the same scale as health care transactions in the medical provider and insurance communities. A workflow management and workstation methodology was introduced to automatically and efficiently present only high-risk transactions to the system for automatic rejection or for review by a fraud analyst.

Unlike the current health IT interoperability flight path, the financial services story of real-time data processing to mitigate fraud did not require a multi-billion-dollar incentive program to get started. However, it did require a first customer, and getting that first customer to pilot the new fraud technology solution was initially difficult. Credit card processors were the first to be approached to launch and pilot the solution, but they declined. They did not have an economic incentive to do so because they were not negatively affected by fraud; they made their revenue by billing their customers for each transaction processed, whether fraud occurred or not. As a normal course of business, they simply raised prices if expenses increased. This is analogous to health insurers raising premiums if they pay fraudulent claims.

The next step was to approach one of the nation's largest credit card issuers to pilot the solution. It accepted the proposal and implemented the system, and the results far exceeded the issuer's expectations. The issuer was able to identify fraudulent transactions that previously would have gone undetected. Its managers were able to implement real-time prevention processes, such as calling consumers, when suspicious purchases were identified.

Because the solution was expensive to implement, it initially met some resistance from credit card issuers. However, as its value was demonstrated to individual issuers, acceptance started to grow. Credit card issuers were discovering that their initial return on investment was generally between 10:1 and 30:1. This means that for every dollar spent on the system, the credit card issuer saved between $10 and $30 in fraud losses avoided. Since the results of the initial implementations were so compelling, other credit card issuers immediately requested to have the solution implemented on their systems. They recognized not only the positive results, but also the

automated infrastructure used to interact with each consumer. Initial fears that the consumers—the credit card account holders—would react negatively to being contacted and asked if they were using their credit card proved to be unfounded. In fact, the approach of calling consumers and stressing the fraud-protection intent of the call became a public-relations success. Today, all credit card issuers use a real-time solution, which includes predictive modeling and workflow management, to prevent fraud within their portfolios.

Lessons Learned from Financial Services

Building an effective fraud-detection system is a continuous learning and improvement process. Each successive system or model enhancement improves upon previous versions. Four lessons learned from the financial services fraud-mitigation experience directly relate to the challenge of implementing health IT systems: (1) the value of real-time assessment; (2) getting accurate data; (3) changing a silo, or isolation, mentality with respect to data sharing and use; and (4) strategies for data integration for rapid use.

Real-Time Assessment. The real-time platform allowed the credit card issuers and their staff to assess and review transactions as they were taking place. Previously, the fraud perpetrators could make a large number of transactions before the fraud was discovered. Now, it is not uncommon to shut down fraud perpetrators as they are attempting their first fraudulent transactions. The financial services industry thus moved from a detection strategy to a prevention strategy. With respect to health care, the value of real-time data emerges in two direct instances: critical care during an emergency and real-time underwriting of future health insurance exchanges.

Accuracy. Initially, credit card issuers were concerned about having to be 100 percent accurate when identifying fraud. This concern was overcome by implementing fraud strategies and processes that ranked the riskiest transactions and then applied the appropriate action or investigation technique to the most questionable transactions. For example, the highest-risk transactions were declined for payment, while other transactions required merchants, via a real-time message, to verify credit card holder identification at the point of sale. The new approach provided a quick and nonobtrusive method to verify whether purchases were authentic. Those transactions identified as less risky were queued for more research and investigated by a fraud analyst. All investigations were online, where previously they were paper-based manual reviews.

While there were always false positives (high-scoring accounts that "looked like" fraud, but were not), the economic benefits of preventing fraud far outweighed any negative impact to accounts that turned out to be nonfraudulent. The legitimate transactions were quickly resolved through customer-service contact. In fact, most credit card issuers used the chance to contact "good" customers as a positive public-relations opportunity, to demonstrate that they were taking action to protect the consumer from fraud.

A similar tradeoff consideration is present for health care, particularly when the data come from insurance billing information. A common concern is that these data are "garbage in, garbage out" because of limitations to the accuracy of diagnostic information. One way this can be addressed is for the medical data recorded at the point of service (similar to the point-of-sale model) to be instantly translated by software into billing data that is later refined to minimize false information about the patient's overall health history. Software like this is used every day by the retail pharmacy industry when drug orders are filled while simultaneously having pharmacists review past drug orders for up to five years to avoid medical errors due to past medical history or concurrent drug use. From the point of view of the financial services industry, there were sufficient incentives to get around complaints that coding was difficult when the benefits far outweighed the costs. In the mid-1990s, retail pharmacies found a way as well—without public financing.

Silo Mentality. Initially, real-time predictive-fraud solutions were implemented at separate credit card

issuer and processor sites. At the time, this seemed to be a natural approach to product market penetration. Later it was learned that this was a less-than-optimal fraud-prevention solution. The ideal solution would have been for all issuers and all processors to have housed their transaction data at a central site.

This has several benefits:

- The ability to capture the history and behavior of the same card holder across all credit card purchases, regardless of the issuer or processor;
- A perspective spanning all issuers and processors to identify fraud rings—after a fraud ring was identified in one portfolio, all other issuers could be alerted, allowing for quicker detection and prevention;
- A comprehensive view of merchants to detect merchant fraud and collusion; and
- A feedback loop across the financial services landscape that allowed the predictive models to learn even more quickly.

Integration. Installing a fraud-detection system into the core of a credit card processor's business-processing system was a long, cumbersome, and expensive proposition. It often took as long as twelve months to implement and test the system. This approach could have been avoided with a modular solution. Under a modular approach, only a data feed would have been required to complete a real-time assessment and communicate back a score, a summary defending the rationale for the score, and a treatment recommendation—a quicker and less expensive pathway to fraud detection.

Parallels to Health Care

Health care and financial services share several opportunities that arise from more effective use of IT. For financial firms, fraud mitigation was a powerful incentive to integrate data, as were ATMs. Once data were organized more centrally in the financial services industry, firms had much better access to data on the performance of retail bank branches and regions. This promoted greater regionalization and later enabled effective nationalization of bank operations. Branch managers were rewarded for better performance in the same way that a hospital CEO could get better payment for performance in a more integrated system. It also became easier to spot weaknesses that needed additional staff to address, as well as opportunities to redirect, reduce, and redeploy staff to different locations. Finally, it made the merger and acquisition process for banks easier at all scales. This is not just a story of Bank of America growing large in the span of fifteen years but also of smaller banks and credit unions that could achieve better economies of scale banding together. In the same way, integrated health IT could empower Accountable Care Organizations and allow smaller physician practices to achieve economies of scale and scope by acquisition from a large hospital with a waiting interoperable health IT technology platform.

The financial services model for mitigating fraud may be more critical to the health care industry as health reform deploys and evolves. Although health care fraud and abuse estimates vary widely, constituents agree that the problem is enormous and growing each year. In testimony before the U.S. Senate Committee on the Judiciary on May 20, 2009, Malcolm K. Sparrow, a prominent expert on fraud, said that health care fraud and abuse costs hundreds of billions of dollars per year, with the actual figure anywhere from $100 billion to $400 or $500 billion.[8] In 2002, a study by the Government Accountability Office estimated that one out of every seven dollars paid to Medicare is lost to fraud.[9] This means that in Medicare alone, there was almost $70 billion in fraud and abuse for 2008 (within a projected $466 billion in total Medicare spending for 2008).[10] Extrapolating this assumption for 2017, Medicare would have over $120 billion in fraud and abuse (within a projected $857 billion in total Medicare spending for 2017).[11] According to experience and research, the vast majority of fraud and nearly all of the abuse is perpetrated by health care providers.[12]

The most common approach in health care fraud and abuse detection today is to apply rules-based or judgmental methodology and technology. Rules are

intended to imitate and automate human judgment. They are typically retrospective "if/then" statements, hard coded into the back end of a claims-adjudication system. The terminology for implementing judgmental criteria is called "edits." This approach also mimics the manual process for identifying claims that are outside of normal policy. But it has done little to mitigate health care fraud and abuse.

Currently, there is no proactive, sophisticated, effective, and efficient fraud-prevention solution in the health care industry.

Today, suspicious claims are paid and reviewed afterward to determine if they violate documented health care policies. If they are found to be questionable, organizations such as Medicare then seek reimbursement through a "pay and chase" strategy. CMS recently started to recover payment errors by using Recovery Audit Contractors. CMS contracts with Recovery Audit Contractors to guard the Medicare Trust Fund. To make a meaningful impact on fraud and abuse in health care, however, new technology and predictive models with real-time assessments must be used to review suspect claims prior to payment.

Currently, there is no proactive, sophisticated, effective, and efficient fraud-prevention solution in the health care industry. Similar to financial services experience in the early days, it is as though no one is "minding the store." However, the recent passage of the Small Business Jobs Act in September 2010 included a provision for full deployment of fraud-mitigation technology by multiple vendors by mid-2011. This component of the bill was introduced by Senator George LeMieux (R-Fla.) and built on four years of Senate interest in advanced fraud-mitigation technology that originated with efforts by Senator Tom Coburn (R-Okla.) and Senator Mel Martinez (R-Fla.). The act creates funding for a real-time claims-data transaction platform that could provide a technology base for national public- and private-insurer data stores similar to what was developed for the financial services industry and is deployed today.

Currently, the financial services industry uses four identical data transaction hubs for financial services that update in real time: Fair Isaac (FICO), TransUnion, Experian, and Equifax. For health care, data that would move in real time would be routed through similar transactions hubs. These data, called "personal health information," would be situated on third-party servers independent of a medical provider or health insurer. Multiple copies of the information provide security, and multiple vendors competing to maintain the contracts promote innovation. The data are also warehoused and can be used as a repository for future research.

In contrast, a handful of states have been creating all-insurance-payer databases for policy research for over a decade with limited success. The data is usually at least a year old, is housed by one vendor, and has little to no value for clinical decision making. Also, new public financing is being made available to Ingenix, a part of UnitedHealth Group—the United States' largest health insurer—to create a national all-payer database for health policy research. This would be the equivalent of Citibank winning a contract to displace FICO and the three other data hubs, with federal financing used to investigate the overall performance of the entire retail banking industry in which Citibank competes. Although UnitedHealth has formidable data-management prowess, it is not nearly as independent as the four transactions hubs built to serve the financial services industry. It also would not deliver real-time information and would require the creation of new public financing.

Toward a Real-Time Health IT System

Achieving interoperability may be too onerous a goal. It is not occurring as naturally as it did in the financial services industry. It is not happening without public financing. And long-term investment in such interoperability—without additional, ongoing public-sector financing—remains in doubt. However, the

recent legislative mandate to use advanced IT for health care fraud mitigation and prevention suggests a different route to real-time health care transactions that could eclipse even the adoption of electronic medical records. Fraud prevention may also prove to be more financially sustainable in health care as a source of funds and innovation, similar to past experience with financial services.

To engage the consumer in the real-time health IT system, a new technology platform needs to be used more broadly. A new technology that could meet this challenge is the Integrated Health Card (IHC). IHC technology is emerging to provide a solution to the problem of combining information from the electronic health record with personal health information. Currently, the technology takes the form of a credit card with a magnetic stripe that identifies an individual at the point of service. Verification of identity is authenticated by queries on date of birth or address. This technology is currently being used for Medicaid eligibility but could easily expand to health insurance claims processing as well. In fact, with respect to pharmaceutical claims processing, the data are currently being used in near–real time between retail pharmacies and pharmaceutical benefits managers.

To be effective, the IHC has to provide value to patients and providers. For patients, it will promptly administer benefits, facilitate health transactions and payments, and thus simplify the process for patients. For providers, the IHC's benefits include prompt payment of claims and access to the patient's pharmacy history and laboratory results. This would be similar to consumer personal-banking dashboards already used for paying bills online or managing one's financial accounts, except that the transactions online would be health records with lab or imaging results to review or share. From a consumer perspective, these services transcend benefit-plan boundaries and traditional geographic limits, enabling patients to have their information follow them across products or across the country.

It remains unclear, however, whether these advantages alone will be sufficient to ensure adoption of IHC technology in the face of provider and patient inertia—not to mention possible resistance from payers who live off the "float" from delaying payment of providers' bills. So far, the IHC platform has been developed by several vendors and used in various public and private insurance settings. For example, the state of Texas is funding an IHC-adoption program for its Medicaid program simply to check eligibility.[13] Several large employers have also deployed various levels of the core components of this technology, including three vendors[14] who already have agreed to provide their technology for free to two demonstration sites to showcase its benefits to patients and providers.

This new technology is significant because its development is based on a currently accepted form of IT, insurance-payment transaction processing. The biggest weakness of a health record built from insurance-transaction data is that the data provided for billing and payment are not complete from a diagnostic perspective. Insurance transactions provide little or no information on simple health-outcome measures, such as laboratory results, and could be biased due to financial incentives inherent in payment rules from public and private insurers. However, these shortcomings are the faults of limited data, not the transaction-based data structure. For example, the Institute of Medicine's advocacy of widespread adoption of computerized physician-order entry systems in 2001 indicates support for a more clinically relevant transaction- or order-based technology platform.

The IHC can also enable speedy health care payments to providers. A 2007 study by McKinsey Consulting found that 90 percent of health care payments require manual interaction, versus less than 1 percent in retail-payment transactions that use card technologies.[15] The "bounce back" of provider-submitted claims to an insurer, where the provider must resubmit the claim, is estimated to be 20 percent to 40 percent, compared to 1 percent of retail transactions. Under an IHC system, provider claims-submission accuracy would approach the retail-sector rate because similar transaction-processing technology would be used. To achieve the performance of the retail sector, provider payment transactions need two critical elements not yet present: a largely electronic payment-submission process

from card technologies (for example, debit cards and gift cards), and an electronic "purse," such as a self-insured company or a state Medicaid program's bank account with American Banking Association routing numbers.

An additional benefit of IHC technology is that it might persuade physicians to add additional data of clinical value to an electronic claims-payment system. The use of an IHC to speed provider payment is a critical issue in this study because accelerating payment for a large share of routine physician services from approximately ninety days to four days could be a significant financial incentive for physician adoption of the technology.

Rapid payment through an IHC could be contingent on the physician's agreement to fill in nonrequired data fields that have high clinical value. The "837" professional electronic claims form used by most public and private insurers already includes the following clinically relevant fields:

- Patient weight at time of service (with the exception of ambulance services)
- Medical record link (possibly an Internet URL for a digital image or lab test)
- Date of onset of current illness

The medical record link could provide a mechanism to identify laboratory values or a link to digital imaging for a radiological service. This information would form the basis of a simple ambulatory medical-records system.

The date/time stamp is an important feature of a transaction-based system because it provides a data-ordering construct for the IHC. For example, if a physician wants to identify a past medical history, he will be looking at the sequence of events as they are recorded by date of service, and, sometimes, over minutes or hours of an emergency or critical-care event. Using the pharmacy date of service, he can see the sequence of prescription drugs a patient was using as well as identify potential problematic drug interactions. The best medical-records systems use time as the central marker for disease progression and health improvement. If the transaction-based system had more clinically relevant and health-outcomes data, it would in fact be a substitute for a computerized physician order entry system, and it could become a full-fledged electronic medical record, complete with date- and time-stamped information that is critical to diagnosis and treatment. If this record allowed the patient to add information to the record, perhaps even on a transaction-specific basis (for example, about a lab test, prescription order, or physician visit), the result would be a very powerful technology.

Innovation

IHC technology is built on one of the most common forms of technology available today: the bank card. As early as 2003, many health plans began issuing "health benefit cards" with bank-card technology, specifically the magnetic strip on the back of the card. In the case of UnitedHealth Group, nearly 20 million members had unique magnetic-strip ID cards by 2006. They could verify eligibility and cost-sharing amounts with a simple swipe of the card if the provider had a common Visa/MasterCard device at the office.

Health insurance claims data comprise the core IT foundation for the IHC. Its architecture is as old as the one used in banking IT, but not nearly as advanced. Banking IT was upgraded in the early 1980s to accommodate the rapid adoption of ATMs. Claims data have not yet been upgraded, and no attempt has been made to make them consumer friendly.

IHC technology can combine both health care and financial information in a single card to support more informed health care consumption and simplify a series of fragmented and time-consuming experiences for health care consumers. Another key goal of the technology is to make an individual's personal health record (PHR) and critical health information highly portable, allowing physicians to have secure access to an online summary of their patients' medical histories. A swipe of the card will call up e-prescribing information not commonly available outside of an integrated delivery system such as Kaiser Permanente

or Intermountain Healthcare. With a patient's permission, the card can also allow physicians to view the patient's PHR, including automatically compiled elements such as a comprehensive summary of medical conditions, medication history, significant medical interventions, and laboratory results. In addition, patients can add information to the PHR such as allergies, immunizations, and family history.

How might this IHC technology operate in an ideal world? Consider a consumer with a chronic illness—diabetes—who has just moved to a new city.

1. On January 1, 2011, she begins health coverage in a new health plan with IHC technology.
2. Before her start date, she receives a health benefit card with a magnetic strip from her employer.
3. Her health plan website provides a list of endocrinologists accepting patients in her area, quality scores for the providers, and indicators for which ones use IHC.[16]
4. She selects an endocrinologist from the list and schedules an appointment for an initial consultation.[17]
5. Before the visit, she logs on to a secure IHC website from the health plan to verify her eligibility and add limited personal health data such as emergency contacts and a "do not resuscitate" order.
6. She also requests that her previous pharmacy history from a different health plan be added to the IHC.[18]
7. When she visits the endocrinologist, the physician's assistant swipes the health card using a USB swipe card reader connected to the Internet with a wholesale price to the physician of five dollars.
8. The swipe opens an IHC page and requests the patient to authenticate her access with a password. She provides the required authentication, followed by approval for the physician to access the IHC.[19]
9. The physician sees on the IHC website that the patient has already authorized him to review her history. He reviews all prior drug history and conducts an initial evaluation of the patient's adherence to critically needed medications, and dosage, previously prescribed for a chronic illness.
10. During the visit, the physician orders blood work for glycosylated hemoglobin, blood sugar, and creatinine. Height, weight, and blood pressure also are recorded on paper records.
11. At the end of the visit, the physician's assistant bills for an initial evaluation on the IHC website. This links to the health plan's transaction engine, which requests standard claims-processing information (for example, diagnosis and procedure codes), as well as the patient's height, weight, and blood pressure. Since this is a standard part of an initial evaluation (signaled by the initial-evaluation code submitted), the website knows to make the request.
12. Since the patient's eligibility information is already known from the initial card swipe and the provider is known to the health plan by being IHC enabled, the allowed amount for the initial consultation is transferred directly to the physician's practice business account. Additional cost sharing (if the patient's plan requires any) is deducted from the checking account or credit card the patient has already entered in her IHC preferences.[20]
13. One day later, the patient receives an e-mail that the lab work has been completed and she can log on to the IHC to see and comment on the results. The physician also receives the e-mail and is invited to comment on the lab results.

14. The patient sees the endocrinologist four more times during the year and keeps recording stable or improving lab values.

15. At the end of year, the health plan invites the patient to comment on quality of care she has received since her HbA1c scores improved. If she comments, she will receive either a reduction in her coinsurance rate or a credit to her health savings account or health reimbursement account if she is enrolled in a consumer directed health plan.

This example highlights how the IHC could work using existing technology platforms. But how might it work with future information technologies? Since all new data—whether discrete data points or streams of data such as biomonitoring—will be time stamped, this technology enables as many different data feeds as are required.

Questions and Concerns

This raises another issue: where do the data actually reside? The best analogy may be the World Wide Web (WWW) as an interface for all data feeds. The Internet functions as a giant network where the user accesses the views she needs. Often, a web page is the product of multiple disparate data sources. The IHC technology is no different: data that are available would need to be accommodated as a live or historic stream. But the platform can make these accommodations as well as any other comparable technology. And WWW does not have to mean "Wild Wild West" with respect to secure transmission of data. In fact, over the last ten years, much if not all corporate financial data moved through corporate intranets that rely on encrypted data streams using the public WWW as an electronic conduit.

Another question arises regarding the use of the IHC technology: are financial services and health information technologies compatible? The idea of fusing electronic medical records and financial transaction systems may seem a bit of a stretch, adding layers of unnecessary complexity. Nevertheless, health insurance data are quite similar to IHC data in three critical areas. First, consumer privacy is paramount in both settings. Second, the structures of the databases are similar in that they both use a debit and credit system to tabulate cash flows and services rendered. Third, both health and financial services data are warehoused for quick storage and retrieval for a variety of different purposes.

To understand the potential for a new real-time transaction model based on an IHC platform, it is important to understand the status quo. Today, the overwhelming majority of health care financial transactions occur through third-party insurers that are private, such as Aetna or Cigna, or public, such as Medicare and Medicaid. The primary business model of third-party insurance is a fee-for-service transaction system between purchasers (employers, governments, and insurers holding risk contracts) and providers of medical care (physicians, hospitals, and pharmacies) on behalf of the patient.

For example, an insured person breaks a leg and goes to the emergency room of a local hospital. The hospital will seek reimbursement from that person's insurer by submitting a claim for reimbursement with specific line items for use of the facility, physician time, medical equipment, pain medications, and x-rays. A consulting orthopedic surgeon, retail pharmacy, anesthesiologist, and radiologist will all invoice separately. The insurer will receive these requests for payment and negotiate final payment over the course of 30 to 120 days following the visit.

Where do banks enter the picture now? If this person works for a large firm that offers health insurance, the firm is likely to be self-insured through the Employee Retirement Income Security Act (ERISA). This firm will likely instruct the insurer to pay the medical providers using the bank account of the employer, following the negotiation of final payments to the providers. Thus, health insurance here is simply "negotiated" fee-for-service. If the injured patient works for a small company that could not afford to be self-insured under ERISA, the payment will originate from the bank account used by the insurer associated with the patient. This would be the case if the patient bought his health insurance in the

individual insurance market as well. If the patient has no insurance and is not in a public insurance program such as Medicare or Medicaid, he would be responsible to pay the hospital charges, which are likely to be at least twice the rate negotiated between the insurers and providers mentioned above. Clearly, the status quo is functional but far from ideal. In fact, the opportunity cost of not moving from the status quo could be staggering if health IT interoperability fails.

Finally, the big elephant in the room is data ownership. Many hands touching health care data believe they own the data, including hospitals and physicians treating patients, insurers processing claims, and even large employers with self-insured contracts. Furthermore, data ownership could be viewed as a source of market power to act monopolistically by creating deliberate barriers to entry and information asymmetry. The good news, given our comparison with the financial services industry, is that banks faced the same challenges over twenty-five years ago as ATMs were adopted. In the end, they made their systems open and got out of the proprietary-data-ownership business. In contrast, the health care industry is comparable to banks in the early- to mid-1970s, with unlinkable data silos and little incentive to link. Different incentives can be put in play if and when trusted third parties step in and start to provide much greater value from the data than one isolated provider or insurer silo could ever provide.

The Perfect Storm Brewing

There is a perfect storm brewing that could radically accelerate the use of real-time transactions and make them the common mechanism of health IT exchange and financing. This acceleration could happen concurrently in the private and public health insurance markets.

Outside of the weather service, the phrase "perfect storm" usually refers to the convergence of two or more trends or powerful forces, people, or factors that can radically alter an environment. In this case, three factors are likely on a collision course. The first is the specter of health reform deployments appearing between now and 2014, depending upon potential adaptations to the legislation following the 2010 and 2012 elections. The second factor is consumers' desire to have information on health providers and services customized to fit their needs. As in the case of online retailing several years ago, early-adopter consumers are willing to trade some privacy for convenience, as trust in health information networks grows. For example, Microsoft's Vault project, as well as the prominent PHR initiative Revolution Health, sponsored by AOL founder Steve Case, may speed up the cultural acceptance of using medical records available on a web portal as consumers trade security concerns for treatment convenience. The third factor is that the evolution of health insurance cards may lead to financial institutions controlling or stewarding health-benefit information flows through the use of existing consumer-transaction platforms, such as credit card data transfer (a widely accepted activity that did not need a publicly financed potential user's conference to gain adoption).

The adoption of a real-time health IT platform could be the key to the insurance-exchange and high-risk-pool health reform initiatives as an enabler of access to insurance coverage. For example, real-time health IT could provide a data repository for health-risk scores that could be used to purchase an insurance policy immediately. This would be equivalent to creating a FICO health score based on everyone's pharmacy history. This is quite easy to do today, and it is already used for underwriting. In addition, the application of tax credits, vouchers, employer-based coverage, or even Medicaid participation could all be accomplished as real-time health IT applications.

Market-Based Health Reform Implementation

Exchanges. Consider the tactical issues involved in implementing the individual mandate authorized by the Patient Protection and Affordable Care Act of 2010 (PPACA). The law requires that almost all individuals purchase insurance or have their employer offer it to them by 2014. Most likely, meeting this

objective will devolve primarily to state-based insurance exchanges. To get such exchanges operational, their administrators can work with one or several technology partners to issue integrated health cards through Visa, MasterCard, or Gratis; everyone in the state receives a card through their health plan, their employer, Medicaid, or social services. This is in fact already happening with food-stamp benefits provided using financial service industry vendors such as the Florida-based FiServ.

To succeed with health IT, we need to go back to the future before "bribed interoperability" became the latest policy prescription.

Underwriting. If every state issues a health insurance exchange identity card, secure web portals or ATMs would be used to authenticate and retrieve an actuarially validated risk score for an individual or family members to price a proposed insurance contract. To do this, data could be extracted from existing retail pharmacy databases to provide information for a predictive model using existing technology from health care actuaries that is based entirely on pharmacy claims. This data would not only describe what drugs a patient takes but how regularly she gets refills, which is highly correlated to chronic-illness management. If a patient managed her illness better, she would get a better risk score and a cheaper insurance policy, just like how driving history or financial credit history informs other insurance underwriting. For an uninsured patient, providers would authenticate the need for care and qualify the patient for a state's pool for uncompensated care. The state-sponsored secure web portal would provide a reported risk score as well as information on available, high-quality providers—both in hospital and outpatient (clinic) settings—customized to a person's condition.

Purchasing Insurance. Next, the state's secure web portal would link to a health insurance exchange provider, such as ehealthinsurance.com, that can create real-time insurance quotes on the exchange and allow consumers to shop for guaranteed-issue plans with premiums reviewed by a certified actuary. Employers would receive notification of their employees' risks as a whole and indicate whether they want to exit the self-insured marketplace if better risk pooling for all their employees exists in the wider market. Many employers such as Caterpillar and 3M are already completing such analyses with internal data. They will use their benefits consulting vendor (for example, Aon Corporation or Mercer) to project their optimal strategy going forward.

Health Policy Surveillance. At the end of the year, the state health department would get health care quality and efficiency reports by different population segments and could identify funding strategies to cover the non-Medicaid uninsured who cannot afford a commercial insurance product. This would enable the state to deliver on the promise for price and quality transparency that has been advocated by the Bush and Obama administrations since 2004.

Dealing Responsibly with Privacy Concerns

Of course, this proposal will not be welcomed by all, even though it could lead to an overall improvement in welfare by removing the current information asymmetry between the provider, the insured, and the insurer that is hobbling the health market. Three substantial issues would need to be overcome. The first is the "privacy sanctuary" claimed by some consumers. A representative of this group might say, "No one should have my information other than me, and I will not share it with anyone for any transaction." If taken to the extreme, this would cause the current system to seize up; consumers would have to live within a cash-only health economy, in which real-time health IT transactions may never be recorded because there is no financial need for electronic financial-transfer intermediation. Medicare and Medicaid, with all their record keeping, could not

exist. This position is likely to be untenable in the long run because of the existing data infrastructure necessary to administer major public health insurance programs.

The key privacy question, however, is access not only to financial data but also to health data, and how that access might be abused by insurers or others. If insurers and banks hope to benefit from the new business model of real-time health IT, they must go to extraordinary lengths to certify the privacy practices of their firms. Some safeguards, dating back seven years, are already in place. For example, the consequences of leaking or abusing personal health information as outlined by the Health Insurance Portability and Accounability Act (HIPAA) involve fines and jail time. The potential for abuse of real-time health IT information for underwriting is the same as for any personal health data. Real-time health IT would increase the velocity and detail of this data, but it would also use digital fingerprints that could make inappropriate behavior easier to identify and prosecute. This would not stop everyone, but it would discourage the exploitation of big expensive holes in the system that may be as common today as they were in the credit card industry fifteen years ago.

The second concern is that the risk rating enabled by new and more current data from real-time health IT could place an unfair burden on the chronically ill. This is potentially a very real concern. However, risk rating should reflect how a person became chronically ill. If behavior (such as smoking, overeating, or alcohol abuse) is the driver for illness, then that patient has become a moral hazard to the health insurance risk pool and should be priced appropriately. One single company, Acxiom Corporation in Conway, Arkansas, has a database combining public and consumer information that covers 95 percent of American households and could be used for a limited form of behavioral risk rating. Insurers could purchase this information, match it to existing or potential contract holders, and examine trends for unhealthy behaviors (for example, unhealthy food habits as recorded through Visa and MasterCard transactions). Having insurers correlate health information with consumer buying information may seem excessive, but it is already being done by, or on behalf of, several employers and insurers that are looking for additional information on patient compliance with diabetes care-management programs.

If, on the other hand, a patient's behavior did not contribute to her major illness, then risk rating should primarily produce a pooling of similar risks for unexpected circumstances—closer to the "pure" insurance models in other industries. This is precisely what happens in the Dutch health care system. Granted, the Dutch government has a stronger role in the health insurance system, but the Swiss also practice risk pooling in a similar way with a less centrally brokered system. Finally, premiums or out-of-pocket payments could be lowered (or taxpayer subsidies through public health programs could be increased) for the chronically ill if they are taking steps to manage their illness.

A third privacy concern involves a potential issue with insurers or other health care providers. They may claim that HIPAA does not permit them to release any health information regarding consumers. However, HIPAA allows consumers to own all their data, including health insurance claims records.[21] As a result, a consumer should be able to go to an insurer, provide a CD or USB thumb drive, and say something like the following: "Download my data, please. Oh, and the data you have archived back ten years, I'd like that too. And, since I'm not sure I'm going to be a member next year, please delete all of the data I'm not using or pay me every time you use it for a commercial purpose without my authorization."

Policy Prescriptions Going Forward

To succeed with health IT, we need to go back to the future before "bribed interoperability" became the latest policy prescription. On its current trajectory, health IT policy is expensive, slow, and likely to be ineffective. In contrast, a market-based approach where incentives align to expand IT functionality for industry and consumers should become the new goal for health IT.

To change the policy, given the current laws of political physics, here is a four-step tactical plan based on the evidence and cases described above.

1. Create at least three financial services hub equivalents for electronic health-claims data today, using all federal and Medicaid data to start. The financial services industry operates with four of these repositories today without federal subsidy. This prescription can be done as part of the modernization of existing technology platforms. Make this part of the health care fraud prevention in the Small Business Jobs Act (signed in September 2010, with implementation in 2011 currently prescribed).
2. Apply existing predictive-modeling technologies for risk assessment in health care to the hub to get a FICO score for all, in as close to real time as possible by also adding real-time retail pharmacy data.
3. Set a goal to pay medical providers at the point of care for all ambulatory services and Medicare-allowed reimbursement less than $3,000, and no more than three days later for all other services. As a fraud-prevention strategy, require lab and imaging tests to be submitted before payment is made. Doing this will turn claims data into electronic medical records within a couple of years, rather than the near-decade that has gone by with almost no tangible progress toward a national interoperable system.
4. Take the ARRA funds and repatriate them to pay for high-risk pools as appropriate to expand coverage for those most in need, as indicated in tactical steps one to three above.

Finally, to show great technical prowess and drive, do all this before the Chinese electronic-health-records system is fully deployed in 2014. Nothing stated above requires more than two years. With motivation, it could be accomplished in one year because it expands on existing best practices that already are being paid for or have the potential to be truly self-financing, if not generate cost savings. That way, whatever the deployment state of the PPACA law, we all will be far better informed with more effective provider and insurance incentives.

Real-time health IT, if widespread, could break the oligopolistic control of health data by providers and insurers.

Conclusion

Real-time health IT, if widespread, could break the oligopolistic control of health data by providers and insurers. In many major metropolitan communities and certainly all rural communities, there are less than a handful of hospitals and insurers in competition with each other. With very rare exceptions, the data necessary to gauge the performance of these institutions is shared neither comprehensively nor at the patient level, as described above. In effect, this data monopoly worsens underlying information asymmetry between providers and insurers and their patient clients. This organizational control results in an information bottleneck that can literally kill patients. But we have other options. Real-time IT is based on a currently accepted form of health IT—insurance payment transaction processing—and could provide a platform to link data across all sites of care without a command-and-control integrated delivery system, creating the information flow necessary for a high-performance medical industry. Of course, this solution ultimately relies on widespread acceptance and wise use of the information by consumers, providers, and financial intermediaries.

Without incorporating alternatives to the health IT government expenditures outlined in the ARRA, the current system will move down a path with many hurdles to surmount, including too much reliance on bribes for an interoperability ideal that may never be fully embraced by the provider community. In contrast, the policy prescriptions outlined above

are pragmatic, based on proven unsubsidized success in the financial services industry, and they could be implemented as part of the routine cost of doing business in the health care industry. This alternate, market-based path can quickly create the health IT platform necessary for transparency in outcomes and performance information for patients, providers, and insurers, private and public alike. There is simply too much at stake for the fiscal and physiological health of the country to pursue the ARRA-fueled path, where the goal of linked medical records becomes plausible only by 2020 or 2030, as opposed to the Institute of Medicine's original goal of 2010.

Notes

1. In fact, the 98,000 estimate was an extrapolation based on three peer-reviewed studies reporting on several hundred patients (mostly based in the New England area), on the improvement in patient safety based on successful deployment of electronic medical records. See Institute of Medicine, *To Err Is Human: Building a Safer Health System* (Washington, DC: National Academies Press, 1999); and Institute of Medicine, *Crossing the Quality Chasm* (Washington, DC: National Academies Press, 2001).

2. By the time Obama took office, ONCHIT was renamed the Office of the National Coordinator (ONC). The reason for the renaming was never explained.

3. Following an initial round of investment as part of the dot-com era, Care-Science Inc. failed to achieve the widespread market share it had hoped to reach based on its business plan.

4. Mary Ellen Schneider, "Internist Faces Challenge as Nation's First Health Technology Czar," *Internal Medicine News*, August 15, 2004, available at www.thefreelibrary.com/Internist+faces+challenges+as+nation%27s+first+health+technology+czar-a0122455017 (accessed November 14, 2010).

5. David Cutler and Mark Pauly, "Will Insurance Reform Bring Down Health Costs?" interview by Kerri Miller, *Midmorning with Kerri Miller*, Minnesota Public Radio, March 31, 2010, available at http://minnesota.publicradio.org/radio/programs/midmorning/?date=03-31-2010 (accessed November 14, 2010).

6. U.S. Government Accountability Office, *Medical Malpractice: Implications of Rising Premiums on Access to Health Care* (Washington, DC, August 2003), 8, available at www.gao.gov/new.items/d03836.pdf (accessed November 14, 2010).

7. U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Activity, "Roundtable: Personal Health Records, Understanding the Evolving Landscape," available at http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID=3169 (accessed November 14, 2010).

8. U.S. Senate Committee on the Judiciary, Subcommittee on Crime and Drugs, *Criminal Prosecution as a Deterrent to Health Care Fraud*, 111th Cong., 1st sess., May 20, 2009, available at http://judiciary.senate.gov/hearings/testimony.cfm?id=3860&wit_id=7953 (accessed November 14, 2010).

9. U.S. Government Accountability Office, *Medicare Fraud and Abuse: DOJ Continues to Promote Compliance with False Claims Act Guidance* (Washington, DC, April 2002), available at www.gao.gov/new.items/d02546.pdf (accessed November 23, 2010).

10. Centers for Medicare and Medicaid Services, *National Health Expenditure Projections 2008–2018* (Washington, DC: U.S. Department of Health and Human Services, 2008), 5, available at www.cms.hhs.gov/NationalHealthExpendData/downloads/proj2008.pdf (accessed November 14, 2010).

11. Ibid.

12. Coalition Against Insurance Fraud, "Go Figure: Fraud Data," available at www.insurancefraud.org/stats.htm (accessed November 14, 2010).

13. Texas Health and Human Services Commission, *Medicaid Eligibility and Health Information Services* (Midland, TX, December 2008), available at www.hhsc.state.tx.us/Contract/529080128/rfp_docs.html (accessed November 14, 2010).

14. For the websites of health IT vendors, go to www.metavante.com (Metavante), www.lighthouse1.com (Lighthouse 1), and www.canopyfi.com (Canopy Financial).

15. Nick A. LeCuyer and Shubham Singhal, "Overhauling the U.S. Health Care Payment System," *McKinsey Quarterly*, June 2007, 3, available at https://www.tipaaa.com/pdf/Overhauling%20the%20US%20Health%20Care%20Payment%20System-McKinsey%20Report.pdf (accessed November 14, 2010).

16. These scores are currently available from many insurers, including the ones participating in this demonstration.

17. This technology is also becoming quite common and is being offered by managed-care plans participating in the study as well as several large multispecialty group practices.

18. This technology is available through RxHub and several state e-prescribing initiatives.

19. An authentication-of-benefits process for social services provided by the state of Minnesota is already being provided to Medicaid-eligible beneficiaries through the participating vendor Medavante.

20. This technology has been offered by Lighthouse 1 to several clients for over two years.

21. Consumers can obtain a copy of the records and limit access to it in certain ways subject to a number of HIPAA exceptions.

1150 Seventeenth Street, NW
Washington, DC 20036
202.862.5800
www.aei.org