July 2012

POLICY INSIGHTS

Government Health Surveillance Vol. 1

National Patient ID

By Twila Brase*

Overview

In 1996, Congress passed a law requiring all American citizens to be issued a national patient identification number.

After a 1998 federal hearing caused a public outcry, Congress prohibited the use of federal dollars to create the unique patient identifier (UPI). However, the law has not been repealed, and in response to new 2009 federal funding to establish a nationwide health information network (NHIN), government agencies, corporations, organizations and the health IT industry have banded together anew to advance a national patient ID card.

The national patient identification system would identify patients, link patient medical records, and allow broad sharing, monitoring, research and analysis of the American public using computerized medical records linked through the NHIN.

Federal regulators may now be attempting an end-run around the 1998 prohibition by funding international projects and by using regulations required under the Patient Protection and Affordable (PPACA) Care Act, the federal health care reform law often referred to as "Obamacare."

Key Points:

- The 1996 HIPAA law requires all Americans to be issued a unique patient identifier (UPI) — a national patient ID card — but a public outcry forced Congress in 1998 to prohibit funding for the ID card.
- There now appear to be attempts to bypass the 1998 prohibition and advance a national patient ID card.
- New federal rules and standardized operations under the PPACA may be an end-run around the prohibition.
- The proposed machine-readable ID card is considered key to accessing and linking patient medical records in the developing Nationwide Health Information Network (NHIN).
- 2.2 million *entities* have access to patient records under HIPAA and the HITECH Act (in 2009 Recovery Act).
- 15 policy proposals are offered to restore citizen rights and patient trust.

161 St. Anthony Ave, Ste 923
St. Paul, MN 55103
www.cchfreedom.org

CITIZENS' COUNCIL FOR Health Freedom
SECURING HEALTH FREEDOM FOR ALL

Specifically, new rules will require healthcare organizations to electronically verify eligibility prior to providing care, will establish a unique *health plan* identifier for use on patient ID cards and will require states to assess and report the health risk status of every individual residing in the state using medical record information, including medical claims data sent to health insurers.

Congress mandated that all citizens be issued a unique patient ID as a passport into the health care system.

There has been little to no discussion of patient consent requirements or potential dangers posed by such a national ID system. Most citizens are unaware of the plan and have long shown opposition to similar proposals when surveyed. This report covers the history and current attempts related to creation of a national patient ID number, which would be used to build a national computerized medical records system without the consent of the public.

Because a confidential patient-doctor relationship is key to patient trust and because patient trust is critical for the frank discussions necessary to receive good medical care, this report also provides policy suggestions for state legislators and members of Congress.

Patient ID Mandate

Most of the American public does not know that Congress has mandated all citizens to be issued a national patient identification number[1] as a passport into the health care system. The government-issued identification, linking and tracking number was enacted nearly 15 years ago through the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The idea was first publicly proposed in the Clinton Health Security Act. Some may recall the national television broadcast on September 22, 1993, where President Bill Clinton held up the National Health Security Card he proposed for all Americans:

> *Under our plan, every American would receive a **health care security card** that will guarantee a comprehensive package of benefits over the course of an entire lifetime, roughly comparable to the benefit package offered by most Fortune 500 companies. This health care security **card** will offer this package of benefits in a way that can never be taken away. So let us agree on this: Whatever else we disagree on, before this Congress finishes its work next year, you will pass and I will sign legislation to guarantee this security to every citizen of this country.*
>
> *With this **card**, if you lose your job or you switch jobs, you're covered. If you leave your job to start a small business, you're covered. If you're an early retiree, you're covered. If someone in your family has unfortunately had an illness that qualifies as a preexisting condition, you're still covered. If you get sick or a member of your family gets sick, even if it's a life-threatening illness, you're covered. And if an insurance company tries to drop you for any reason, you will still be covered, because that will be illegal. This **card** will give comprehensive coverage. It will cover people for hospital care, doctor visits, emergency and lab services, diagnostic services like Pap smears and mammograms and cholesterol tests, substance abuse, and mental health treatment.[2] [Emphasis added]*

Although Clinton's plan to nationalize health care failed, his plan for a national health data system and a national patient ID card continues to advance outside the public's awareness.

HIPAA, enacted August 21, 1996 requires the U.S. Department of Health and Human Services (HHS) to issue to every citizen a Unique Patient Identifier (UPI)—a national patient ID number. It also requires HHS to issue a National Provider Identifier (NPI) to all doctors, clinics, hospitals and other practitioners.[3] Several "enumerators" have been set up across the country to enroll practitioners and facilities into the National Provider Identification system.

The ultimate goal is accurate identification and the linking of all related information to that individual.

In addition, a Unique Health Plan Identifier (HPID) for managed care plans and health insurers as well as a unique employer ID number for employers were enacted. The NPI regulation was adopted October 16, 2002, and the longstanding federal Employer Identification Number (EIN) was selected as the employer identifier in 2004.[4] Federal regulations to issue the HPID are currently being written and must be promulgated by October 1, 2012.[5, 6]

Specifically, the 1996 law required the Secretary of HHS to adopt certain health care transaction standards by February 21, 1998, including the provision of a "unique health identifier for each individual, employer, health plan and health care provider for use in the health care system."[7]

"The ultimate goal," according to the Healthcare Information and Management Systems Society (HIMSS), "is the accurate identification of the patient and linking of all related information to that individual within and across systems."[8] Although the industry supports this goal, many individuals in the general public feel quite differently.

Funding Prohibited

The Congressional mandate for a national patient ID number has proven to be quite controversial. In 1998, two years after HIPAA passed, the National Committee on Vital Health Statistics (NCVHS) scheduled a series of public hearings nationwide to discuss the Unique Patient Identifier. The first hearing took place that July in Chicago. I testified against the UPI.[9] The next day, *The New York Times* reported the hearing on its front page, raising the public's ire. On July 31, HHS announced a delay in implementation and no more hearings were held.

Shortly thereafter, Congressman Ron Paul, MD (R-TX), added language to a 1998 budget bill to prohibit federal funds from being used to create the UPI:

> *None of the funds made available in this Act may be used to promulgate or adopt any final standard under section 1173(b) of the Social Security Act (42 U.S.C. 1320d–2(b)) providing for, or providing for the assignment of, a unique health identifier for an individual (except in an individual's capacity as an employer or a health care provider), until legislation is enacted specifically approving the standard.*[10]

This also means "no federal resources will even be put into investigations of national

health care identifiers," says Barry Hieb, M.D. chief scientist of Global Patient Identifiers Inc. in Tucson.[11] The prohibition has even led some federal officials to say, "We can't talk,"[12] when someone wants to discuss national patient identifiers.

State and other efforts to establish the UPI are very much alive.

The Rand Corporation, in a 2008 study funded by a consortium of health information technology companies (Cerner Corporation, CPSI, Intel, IBM, Microsoft, MISYS, Oracle, and Siemens), decries the nation's lack of progress toward a national UPI:

> *[U]nlike almost all of the other governments, Washington is not developing a unique patient identifier to use as a* ***singular key to accurately link, file, and retrieve*** *individual health records.*
>
> *Privacy and security concerns have* ***completely sidetracked*** *the development of a UPI for individuals in the United States …. Although an analysis completed for HHS in 1997 suggested a number of practicable options for a* ***national patient identifier,*** *subsequent hearings conducted by the National Committee on Vital and Health Statistics (NCVHS, 1998) revealed significant concerns that the privacy and security of patient information could be threatened if it were networked beyond local health care information systems ….*
>
> *Congress subsequently prohibited HHS from expending funds in a further study of a UPI without its explicit approval. This prohibition effectively stopped HHS from further considering or experimenting with a UPI as a means of linking health information in a national or regional network.*[13] *[Emphasis added]*

Congressman Paul's prohibition remains in law today, but the national patient identification number is not dead. In fact, state and other efforts to establish the UPI are very much alive.

Out of Africa—SmartCare

The U.S. Department of Health and Human Services used federal funds to create a patient identification system and ID card across the ocean—in Africa. When Secretary of State Hillary Clinton visited Zambia, "she praised the government for its vision in deploying an electronic health record system that stores a person's data on a pocket-sized plastic card."[14]

Mrs. Clinton told an audience at a university hospital in Lusaka that she had tried unsuccessfully for a decade to get a similar system in place in the United States. A news report features a photo of Mrs. Clinton standing at a podium holding up the SmartCare card. Mrs. Clinton concluded, "So I may need to send some people here to see how it is done."[15]

SmartCare, funded by the U.S. Centers for Disease Control (CDC), a division of the U.S. Department of Health and Human Services, is a national electronic patient identification and medical records card.[16] SmartCare is called "one of the largest nationwide electronic medical record system [sic] in Africa."[17] Perhaps as an inducement, clinics in Zambia are now required to install SmartCare to dispense anti-viral HIV drugs,[18] most of which are likely funded and provided by the United States.

Using federal taxpayer dollars provided by the CDC, SmartCare began in 2005 as a pilot project of Jhpiego (pronounced "ja-pie-go"), an affiliate of Johns Hopkins University. SmartCare was developed to provide "timely data" on various diseases and maternal and child health for public health purposes, including "trend reporting and analysis of health officials and clinicians."[19]

SmartCare card carries an encrypted copy of a patient's entire health history.

According to Jhpiego, the seamless data interaction between the SmartCare card and the established paper card "facilitate the national rollout of the system and a smooth transition, over several years of implementation, from a paper-based system to an electronic one."[20] According to Dimagi, a "privately held software consultancy founded in 2002,"[21] headquartered in Cambridge, Massachusetts:

> *SmartCare is a U.S. Centers for Disease Control (CDC-Zambia) initiated nationally scalable Electronic Health Record System designed specifically for low resource, disconnected settings. SmartCare has the objective of improving the quality of health care (and health) by providing support o [sic] deliver [sic] "Continuity of Care" where existing paper systems are failing to preserve a longitudinal data view, and where clinics may often have no telecommunications.*
>
> *SmartCare supports longitudinal record-keeping for a variety of health verticals, including HIV/AIDS treatment, TB care, VCT [Voluntary Counseling and Testing for HIV/AIDS], and antenatal care. It provides clinical decision support, touchscreen interaction, off-line data synchronization, and data portability via the use of smart cards.…*
>
> *Dimagi began working with the Centers for Disease Control and Prevention in Zambia in 2004 to design a country-wide smart card based EMR and HMIS [Health Management Information System] system. The objective of the project was to track patient information across rural and urban clinics in order to improve continuity of care for the patients and providers, as well as to strengthen the HMIS capacity of the country.*
>
> *SmartCare currently holds over 250,000 patient records, and is in 459 clinics in all 72 districts in Zambia, making it the largest system of its kind in Africa.*[22]

The SmartCare card is:

> *a key part of the electronic health record system. This customized card carries an encrypted copy of a **patient's entire health history**. … Health records travel directly with the patient. A soft copy of the health record is saved in the SmartCare database of every facility the patient visits. These data are later de-identified, and pooled at the district, provincial and national levels for public health monitoring, evaluation and HMIS use."*[23] *[Emphasis added]*

State Identifiers?

While the federal government is prohibited from expending funds to establish a federal

patient ID, the 50 states are not. For example, the 2009 Nevada legislature passed a bill requiring the state health department:

> *[I]n cooperation with medical facilities, providers of health care and any agency of the Federal Government, [to] investigate options for creating a unique patient identification mechanism to allow a patient to be identified from one facility or provider to another without requiring the disclosure of a social security number.*[24]

Nevada rejects the Social Security Number as UPI, but Minnesota adopts the SSN.

Although Nevada does not yet appear to have adopted a state patient ID system, a 2011 state law requires patient safety policies for health care facilities, including "a policy for appropriately identifying a patient before providing treatment, such a policy must require the patient to be identified with at least two personal identifiers before each interaction with a health care provider, the personal identifiers may include, the name and birth date of the patient."[25]

Minnesota went further. In 1994, shortly after the demise of the Clinton Health Security Act—and before the Act's Administrative Simplification language was enacted through HIPAA—Minnesota legislators required unique identifiers for patients, health insurers, practitioners and employers. The state's UPI language was clear:

> *On and after January 1, 1996, all group purchasers and health care providers in Minnesota shall use a unique identification number to identify each patient who receives health care services in Minnesota …. The social security number of the patient shall be used as the unique patient identification number …. The unique patient identification number shall be used … for purposes of submitting and receiving claims, and in conjunction with* ***other data collection and reporting functions*** *…. The commissioner shall develop an alternate numbering system for patients who do not have or refuse to provide a social security number…*[26] *[Emphasis added]*

After the passage of HIPAA in 1996, the Minnesota legislature revised the state statute language to conform to the UPI language in federal Title 42 of HIPAA. However, the language allows the state to create an alternative numbering system for patients, but only "within the limits of available appropriations" and only if federal law allows it:

> *The unique health identifier for individuals adopted or established by the federal Secretary of Health and Human Services under United States Code, title 42, sections 1320d to 1320d-8 (1996 and subsequent amendments), shall be used as the unique patient identification number …*[27]

Not the SSN

In the early 1990s, shortly before the introduction of the Clinton Health Security Act, the American College of Medical Informatics began discussing how to identify patient records and recommended adoption of the Social Security Number (SSN). This proposal did not sit well

with everyone involved in the organization. Two concerned individuals wrote a paper titled, "Against Simple Universal Health-Care Identifiers." Peter Szolovits and Isaac Kohane caution:

> *If we organize our records in such a way that the indexing of information is routine, then we make the **job of the snoop** much simpler and less expensive .... [Emphasis added]*
>
> *...[U]nder current proposals, we are making it simpler to collate information from very different sources by indexing all transactions pertaining to an individual under his or her SSN. Future snoops may be able to develop lists of people with certain educational and job backgrounds who suffer from specific maladies and like to spend money on certain kinds of entertainment. The opportunities for abuse are enormous. Yet the more and more widespread adoption of a single identifier facilitates and encourages just this situation. ...*
>
> *Originally limited in use to recording individual contributions to the social security plan, its approved Federal use has been broadened to identifying taxpayers and their tax transactions, civil service employment, Defense Department personnel, recipients of some forms of public assistance, and other functions. In addition, states use the SSN for their own tax-related records, and may also index drivers' licenses, motor vehicle registration, and criminal history to the same identifier. Non-government uses include records holding an individual's history of employment, insurance, credit, and education. If current trends continue, health records will join this list. [NOTE: Medicare cards use the full SSN.[28]]*
>
> *With growing interoperability of database systems, we are getting close to the time when a single SQL [Structured Query Language] query can, at not very great cost, find a selection of individuals based on any or all of the characteristics indexed by the SSN… To anyone who values privacy even slightly, this is a frightening prospect.[29]*

"To anyone who values privacy even slightly, this is a frightening prospect."

Patients Want Privacy

A medical record "may contain more intimate details about an individual than could be found in any single document,"[30] yet proponents of a national patient ID envision access to a patient's entire medical record, regardless of its location. Dr. Rob Bush, president of Orchard Software, says, "Access to a complete set of medical records means every doctor has the potential to see all our records and do a better job of treating us."[31]

According to the NCVHS, "A patient identifier that is unique ***across the entire national healthcare system*** will facilitate an easy implementation, reduce cost and complexity, and assure timely access to information for patient care, administrative and research purposes." In other words, per NCVHS, "A Unique Patient Identifier has the potential to assure prompt access to healthcare information, timely delivery of care, ***linkage of lifelong health records*** of individuals, aggregation of health information for analysis and research."[32] [Emphasis added]

Many in the public do not share the view of the National Committee on Vital Health Statistics. A 2000 Gallup poll conducted before most Americans were thinking of electronic medical records, and before privacy breaches became headline news, found the following:

- 88% opposed requiring all patient medical records to be stored in a national computerized database over their lifetime;
- 87% were not aware of the federal plan to assign medical identification numbers; and
- 91% opposed requiring a medical identification number to track medical records and place them in a national computer database without the person's permission.[33]

42% believe "privacy risks outweigh expected benefits."

Nor do Americans want every doctor, hospital, health plan, researcher and public health department to have access to their entire medical record. The Gallup poll looked at nine categories of groups. Citizen opposition ranged from 95% being opposed to banks accessing medical records without consent to 59% opposing pharmacist access to medical records without consent. For example,

- 92% opposed allowing government agencies to access medical records without consent;
- 84% opposed employer access to medical records without consent;
- 82% opposed insurer access to medical records without consent; and
- 67% opposed allowing researchers to access medical records without consent.[34]

The public has remained strongly supportive of privacy protections for private medical record data. A 2006 Harris poll found only 29% of the public expecting the benefit of electronic medical records to outweigh the privacy risks.[35] More importantly,

- 42% believe "privacy risks outweigh expected benefits";
- 29% say they are not sure how they feel about privacy risk vs. EHR benefits; and
- only 26% knew anything about plans to build a national health information network (NHIN).[36]

Although patients may not know about the ongoing attempts to create a national medical ID and a national medical records system, some who actually get a copy of their medical records have been given new reasons to support privacy and patient control over the data.

Many have been surprised and upset by what they find written in their medical record. Innocent conversational details about home and family relationships have been included and erroneous diagnoses have been entered.[37] Scrubbing the record of details the patient never intended to share broadly may prove all but impossible once the data is electronically available and online.

Other patients may want to control access to secure a fresh and completely unbiased second or even third opinion. They may also want to protect themselves from becoming an involuntary research subject. A national unique patient identifier threatens the ability of these individuals to meet their needs and limit their exposure to unwanted uses and disclosures.

Right to Privacy

Citizens also have a constitutional right to privacy. Yet, according to the federal government, the HIPAA "Privacy" Rule, in combination with the HITECH Act within the American Recovery and Reinvestment Act ("economic stimulus") gives ***2.2 million entities***, including various government agencies, access to private medical records without patient consent.[38] This is a violation of individual rights under the Constitution of the United States of America. According to Betty M. Ng, writing in *Rutgers Computer and Technology Law Journal*, "The right to privacy has been found in the First, Fourth, and Fifth Amendments, as well as the Fourteenth Amendment's notion of personal liberty."[39] The Fourth Amendment of the U.S. Constitution specifically states:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

"Every unjustifiable intrusion by the Goverment must be deemed a violation of the Fourth Amendment."

In *Katz vs. United States*, a lawsuit over government wiretapping, the U.S. Supreme Court found "constitutional protection must be accorded to a person who justifiably relies upon the privacy of a particular place, be it a home, office, car, or telephone booth."[40]

Supreme Court Justice Louis Brandeis, in an earlier case of federal wiretapping, wrote, "Every unjustifiable intrusion by the Government upon the privacy of the individual … must be deemed a violation of the Fourth Amendment."[41] He also warned that scientific progress could potentially lead to greater governmental intrusion into private lives.[42]

Functions of Patient ID

Leading proponents of the Unique Patient Identifier focus on the identification system—and steer clear of individual rights. "The primary focus of healthcare is shifting from treatment of diseases to disease prevention and promotion of health and wellness through consumer education. The health information will cover the ***entire life span of an individual***. The health record of an individual may begin with ***genetic and prenatal*** data and end with that individual's death,"[43] declares the National Committee on Vital Health Statistics (NCVHS), a group that by statute must advise the Secretary of the U.S. Department of Health and Human Services on data initiatives in health care. [Emphasis added]

NCVHS says the Unique Patient Identifier must support four basic functions, including purposes not directly associated with patient care:

1. Identification of an Individual
    a. for the purposes of delivery of care (diagnosis, treatment, blood transfusion, medication, etc.)

b. for administrative functions (e.g. eligibility, reimbursement, billing, payment, etc.)

2. Identification of Information

   a. Identification and access to patient information for prompt delivery of care during current encounter, coordination of multi-disciplinary patient care services and communication of orders, results, supplies, etc.

   b. Organization of patient care information into a manual medical record chart or an automated electronic medical record for both current and future use

   c. Manual and automated linkage of various clinical records pertaining to a patient from different practitioners, sites of care and times to form a ***lifelong view*** of the patient's record and facilitate the continuity of care in future

   d. Aggregation of information across institutional boundaries for population-based research and planning

3. Accurate identification functions (to provide timely access to patient care information) and disidentification functions (to support the protection of security, privacy and confidentiality of patient information)

4. Reduce healthcare operational cost and enhance the ***health status of the nation*** by supporting both automated and manual patient record management, access to care and information sharing.[44] [Emphasis added]

The ID card is key to accessing individual EHRs stored in the Nationwide Health Information Network (NHIN).

No Card. No Care?

A unique identification *number* allows tracking and linking. The citizen's medical record ID number will be embedded in a unique identification *card*. If patients are required to present a national patient ID card with a national patient identification, tracking and linking number for access to health care services, the patient's right to privacy and autonomy is violated. If the patient's medical data can be further accessed by the federal government, as is allowed under the so-called HIPAA "Privacy" Rule, the citizens' constitutional right to privacy is violated.

Congressman Dick Armey (R-TX) once said, "[W]e didn't beat back the administration's plan to issue us all 'health security cards' only to have Congress adopt an I.D. card to track down immigrants."[45] Yet the national patient ID has been slowly advancing behind the scenes.

For example, a 2011 federal health reform rule requires most[46] healthcare providers and organizations to check patients' insurance eligibility and financial responsibility prior to, or at the point of, receiving health care services.[47] Compliance is required by January 1, 2013. The rule, issued July 20, 2011, supports the health insurance industry's long-term goal of incrementally moving toward electronic health ID cards for all Americans.[48]

The proposed machine-readable ID card would serve as the key to accessing individuals'

electronic health records (EHRs) stored in the Nationwide Health Information Network (NHIN)—a "network of networks"[49] used to access patients' medical records. In 2006, NHINWatch.com reported:

> *WEDI, the Workgroup for Electronic Data Interchange, has been steadily and quietly working on … health identification cards …. WEDI's work is critical to the building of the infrastructure of the national health information network (NHIN).*
>
> *What's the connection between a standardized health ID card and NHIN? One key WEDI discussion has revolved around what in fact a health ID card will do ... the health ID card [will be] a "token" or a gateway to access the NHIN,* ***a way to reach all the databases that store a patient's clinical information****, but with the capability of being able to block off certain information from access. …"The card itself is an ID card that gets you to the gateway [for access to not only financial resources but a "payer-based health record"]... and can help you access data."*[50] *[Emphasis added]*

Health ID cards might become mandatory for patients in the future.

Meanwhile, in 2009 the Medical Group Management Association (MGMA) "launched Project SwipeIT … to push for full implementation of magnetic insurance ID cards in all public and private health insurance plans."[51] *ModernHealthCare.com* noted:

> *A few years ago … many stakeholders were talking about using "smart cards" where a patient's records were stored on a chip, but that required medical providers to have the technology on hand to access the chip and update that stand-alone file. Instead, the cards the MGMA is now promoting … contain only the most basic information and function as a key to enter a Web-based portal—known as Availity—where patient information is kept …. [T]he MGMA is calling for stakeholders to follow the WEDI playbook.*[52]

In February, 2011, WEDI approved its "Health Identification Card Implementation Guide." The guide recommends various types of health ID cards, including permitting, but not requiring, one that combines health insurance and banking (credit or debit card) information.[53] WEDI also notes, "2010 Federal legislation permits standardization of health insurance and benefit cards. So it may happen that, while this guide is currently voluntary, it might become ***mandatory in the future***."[54] [Emphasis added]

MGMA has also stressed, "Without strong consensus and commitment from all major insurers—or an ***unequivocal federal mandate***—individual plans have been unwilling to take the first steps and implement their own swipe cards. And if the plans weren't going there, neither would physicians, even though both parties stand to gain."[55] [Emphasis added]

In a letter to HHS Secretary Sebelius, and in support of "industry momentum toward adoption of a machine-readable standardized patient ID cards [sic]," WEDI leadership wrote:

> *We understand there is an estimated* ***25 to 30 million*** *machine-readable patient ID cards already in circulation that conform to the WEDI Health Identification Card Implementation Guide and use this format for the health plan identifier.*[56] *[Emphasis added]*

"Exchange" ID Card

States to collect risk-related data to determine individual risk scores.

The Patient Protection and Affordable Care Act (PPACA - *Public Law 111-148*) says all 50 states "shall" establish an American Health Benefit Exchange that complies with all federal PPACA exchange regulations. If a state refuses, the PPACA authorizes the U.S. Department of Health and Human Services (HHS) to establish and operate such an Exchange within the state that complies with all federal Exchange regulations. Under the law, Exchanges are required to oversee the entire health care industry—insurance and the delivery of medical care—and report to the federal government.

The national patient ID is key to the data sharing required between the Exchange and the federal government. A recently proposed federal rule provides just one example of private data that will be shared. The 2011 proposed PPACA "Reinsurance, Risk Corridors and Risk Adjustment" (3R) Rule would require states, or the federal government on behalf of states, to "collect risk-related data to determine individual risk scores that form the basis for risk adjustment" within the health insurance exchanges. Such data includes "claims and encounter data" and "demographic and enrollment data."[57]

While HHS in the 2012 final "3R" Rule forbids collection of names, or storage of any personally identifiable information as a unique identifier unless encrypted or masked,[58] HHS initially proposed ***three methods to collect risk scores created on individual citizens***:

> *(1) a centralized approach in which issuers submit raw [medical] claims data sets to HHS; (2) an intermediate State-level approach in which issuers submit raw claims data sets to the State government, or the entity responsible for administering the risk adjustment process at the State level; and (3) a distributed approach in which each issuer must reformat its own data to map correctly to the risk assessment database and then pass on self-determined individual risk scores and plan averages to the entity responsible for assessing risk adjustment charges and payments.*[59]

This approach has also been discussed in a paper published by the American Enterprise Institute and written by Stephen T. Parente, PhD, MPH, MS, and an AEI adjunct scholar. In *"Harnessing Health Information in Real Time: Back to the Future for a More Practical and Effective Infrastructure,"* a broad range of ideas are suggested including:

- assigning every American a risk score — a "FICO score for all"
- mining patients' retail pharmacy data for scores "as close to real time as possible"
- developing three transaction hubs nationwide on "third-party servers independent of a medical provider or health insurer" for warehousing medical claims data
- allowing the warehoused data to "be used as a repository for future research"
- creating ***"integrated health cards"*** *(IHC) for patients* [Emphasis added]
- "fusing electronic medical records and financial transaction systems" through the IHC.[60]

Mr. Parente writes, "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." In the same report, he also states:

> *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 ...*
>
> *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) ...*[61] *[Emphasis added]*

Databases combining public and consumer information could be used for behavioral risk rating.

Industry End-Run

Although Congressman Ron Paul has effectively prohibited the creation of a national patient ID number by the federal government for 14 years, at least ***three new industry developments*** threaten to undo his efforts to protect patient privacy and consent rights.

First, the health information technology industry, long involved as members in the Workgroup on Electronic Data Interchange (WEDI), is lobbying Congress to repeal the federal moratorium on funding for unique health identifiers for individuals:

> *In September, HIMSS [the Healthcare Information and Management Systems Society] specifically recommended in its federal policy agenda that Congress support the development of a "nationwide patient identity solution." Doing so, according to HIMSS, could be accomplished by lifting a provision in the 1999 Omnibus Appropriations Act (that has been carried forward in all subsequent appropriations bills) prohibiting the use of federal funds to "promulgate or adopt any final standard" for a unique patient identifier until Congress enacts legislation specifically approving a standard.*[62]

Second, the recently proposed rule on the national Unique Health Plan Identifier[63] may be used to standardize patient identification cards nationwide. According to a letter to HHS Secretary Sebelius written by WEDI, whose members include health plans, government agencies and health information technology (health IT) corporations, the group states:

> *This advisory ... addresses our concern that without clarification on two aspects of the*

HPID [Unique Health Plan Identifier], further release of machine-readable standardized patient identification (ID) cards could be impeded.[64]

Machine-readable health ID cards easily capture and accurately transmit patient demographic and insurance information.

Third, the PPACA requirement for standardized operating rules for health plans appears to be a less than obvious end-run around Congressman Paul's prohibition on creation of a national patient ID. By all appearances, it is leading to standardized patient ID cards issued by health plans. By requiring health care organizations to check the eligibility and financial responsibility requirements of each patient prior to providing access to health care services, the regulation moves toward a ***defacto national patient ID system***.

The HHS regulation, finalized on December 7, 2011, implements the first two phases of a three-phase incremental approach created by the Council for Affordable Quality Healthcare (CAQH), a nonprofit industry group affiliated with America's Health Insurance Plans.[65] CAQH established a Committee on Operating Rules for Information Exchange (CORE) to facilitate ***real-time data exchange*** for health plans and providers.[66]

The National Committee on Vital and Health Statistics (NCVHS), which is required by statute to advise the Secretary of HHS on "health data, statistics, and national health information"[67] has recommended that CORE be the author of the nation's operating rules related to pharmacy-related transactions for eligibility, claims status and electronic remittance advice.[68] Finalized and forthcoming rules from this industry group include three phases:

- CORE Phase I Rules—focus on "real time electronic eligibility and benefits verification, as eligibility is the first transaction in the claims process," notes CORE.
- CORE Phase II Rules—focus on electronic eligibility by adding additional data content requirements that provide patient financial liability information (i.e., patient out-of-pocket expenses).
- CORE Phase III Rule—establish basic minimum ***requirements for issuers of health insurance identification cards***.[69] [Emphasis added]

The Medical Group Management Association (MGMA) claims HHS operating rules "may allow for the use of a machine readable identification card." In support of national rules related to insurance-issued patient ID cards, a MGMA publication states:

... machine-readable health ID cards have the potential to easily capture and accurately transmit patient demographic and insurance information directly into the provider's electronic patient management system (e.g. practice management system electronic health record, hospital-based record, etc.), which in turn is used to ultimately generate and track patients' claims. Named in HIPAA as an advisor to the Secretary, the Workgroup for Electronic Data Interchange (WEDI) has developed specifications for machine-readable ID cards as well as required data elements to be included on the physical cards.[70]

According to CORE documents, phase three includes an "ID Card" for patient identification.[71] What's more, ***"CORE rules will support the guiding principles of the***

NHIN."[72] [Emphasis added] As CORE's managing director testified in April, 2010, before the NCVHS Subcommittee on Standards:

> *It is not news to any of us that the delivery of healthcare is evolving at a new rate of speed. Only a decade ago we were discussing processes for electronic claims submission, and over the past few years, the Office of the National Coordinator for Health Information Technology (ONC)* ***created the Nationwide Health Information Network (NHIN)***[73] *... [O]ver the last year, CAQH CORE staff has been frequently meeting via conference call with [federal] staff members ... who are working to address the administrative data exchange priorities of the NHIN.*[74] *[Emphasis added]*

Patient IDs are the "linchpin" to making electronic health data systems interoperable.

The "Workaround"

Industry proponents of a national patient ID abound. According to Raymond D. Aller, MD, director of automated disease surveillance systems for Los Angeles County, "the lack of a uniform patient identifier is the No. 1 clinical informatics problem in this country."[75] More strongly put, ***"[I]t's the linchpin to making [data] systems interoperable,***"[76] says J. Mark Tuthill, MD.

Today the industry's "workaround" solution for identifying one John Jones from another John Jones is the Enterprise Master Patient Identifier, or EMPI, for which Wikipedia has a concise definition:

> *In computing, an Enterprise Master Patient Index (EMPI) is a form of Customer Data Integration (CDI) specific to the healthcare industry. Healthcare organizations or groups of them will implement EMPI to identify, match, merge, de-duplicate, and cleanse patient records to create a master index that may be used to obtain a complete and single view of a patient. The EMPI will create a unique identifier for each patient and maintain a mapping to the identifiers used in each records' respective system.*[77]

According to Dr. Aller, "The computer [EMPI system] pulls together all kinds of different identifiers like birthdate, address, the spelling of the name, and the sound of the names."[78] The EMPI's demographic match and calculated guess for identifying the correct patient in the database are accurate approximately 92 to 96 percent of the time.

The industry reports that these errors have a financial cost. According to the American Health Information Management Association (AHIMA), "Industry experts estimate current organizational MPI error rates are between 7 percent and 10 percent and cost between $10 and $20 per duplicate to correct. To put the duplicate MPI problem in proper perspective, if the organization has 300,000 patients in the MPI, there could be 30,000 duplicates, which, in turn, cost the organization $60,000."[79]

Voluntary ID System?

Patient trust will be jeopardized by a national identification and tracking number.

In response to privacy concerns over a government-issued national patient ID, Global Patient Identifiers Inc. (GPII) in Tucson, Arizona, introduced a Voluntary Universal Healthcare Identifier (VUHID) in 2009 "that represents 24 years of development work."[80]

GPII's chief scientist, Barry Hieb, MD, who testified at the 1998 Chicago hearing in support of using both the EMPI *and* a national health care identifier to "facilitate linking information from disparate sources into a single, comprehensive, consistent record …[81] says of VUHID, "The system would enable unambiguous patient identification, error-free linkage of clinical information, and enhanced privacy of patient information."[82]

GPII's goal is to "make unique healthcare identifiers available to any patient who uses the services of a regional health information organization (RHIO) or health information exchange (HIE) …." The VUHID is:

> *a voluntary system of assigning patient IDs that manages to sidestep most of the objections that have stymied a national system so far.… The system's goal is to make unique health care identifiers available at nominal cost to individuals who want one. But more than that, VUHID promises to shield patient privacy by using two categories of identifier: an open identifier for information a person wants to have known to all of his or her care providers, and multiple private identifiers for medical information a person wants to keep private.*[83]

Although GPII wants to "engage the health care privacy community in an active dialogue," its view of privacy appears to rest solely within the National Health Information Network. They are not opposing the NHIN. Instead, GPII plans to "enhance the privacy capabilities of the nationwide health information network."[84] Whatever GPII's intentions, it has received funding from the Robert Wood Johnson Foundation, an advocate for universal coverage.

Policy Proposals

Patient trust is key to good medical care.[85] A 1999 California HealthCare Foundation study found 15 percent of people delaying medical care, asking doctors to omit information, or falsifying data to protect their own privacy.[86] Infringing on medical privacy harms patients. Approximately 586,000 people per year avoid early diagnosis for cancer alone.[87] Patient trust will be jeopardized by the continued advance of a national patient ID for building a national computerized medical records system of linked and broadly accessible private medical records.

Since the 1996 federal HIPAA law and the 2000 final HIPAA "privacy" Rule ***allow stronger, more privacy-protecting state laws to supercede the HIPAA law and rule***, state legislators and Members of Congress may wish to consider the following policy proposals:

1. Prohibit implementation of a national patient ID number, card or system.

2. Repeal the Unique Patient Identifier and other HIPAA-imposed IDs from federal law.

3. Prohibit implementation of a state patient ID number, card or system.
4. Prohibit required use of any identification card for patients who pay cash.
5. Require informed written patient consent for placement of medical records into an online, interoperable electronic medical records system.
6. Require informed written patient consent for placement of medical records into a state or regional Health Information Exchange (HIE).
7. Repeal and defund the national health data system, now called the Nationwide Health Information Network (NHIN).
8. Repeal state laws requiring use of interoperable electronic medical record systems.
9. Repeal state and federal laws penalizing practitioners for failure to install interoperable electronic medical record systems.
10. Repeal e-prescribing mandates at the state and federal levels.
11. Restore longstanding informed written patient consent requirements for the sharing and use of patient data and medical records.
12. Require patient-accessible audit trails that log and track all accesses to interoperable electronic medical record systems, including government agencies, law enforcement, researchers, and payment, treatment and health care operations.
13. Impose civil and monetary penalties for violation of informed written patient consent requirements.
14. Rescind the U.S. Department of Health and Human Services' March 23, 2012 final rule, "Patient Protection and Affordable Care Act; Standards Related to Reinsurance, Risk Corridors and Risk Adjustment," which requires, among other things, collection and submission of data regarding "determination of an individual's risk score..."
15. Establish patient ownership of medical record information in state and federal law.

Patients have a right to privacy of medical data and the details of their personal lives.

Conclusion

Under the U.S. Constitution, patients have a right to privacy. Patients also desire privacy and personal control over their medical information. However, federal and state laws are advancing a national patient identification system that will allow all medical records to be linked into a lifelong, longitudinal record of all patient encounters with any health care system in the country and available to 2.2 million entities, including government officials without patient consent.

Data linked by the citizens' national patient ID number could include demographic data, diagnoses, genetic code, family relationships, treatments, personal comments, hospitalizations,

behaviors, lifestyles, dates and times of service, phone calls, names and actions of physicians and other clinical personnel, type of insurance, name of insurer and myriad other data.

The implementation of the Unique Patient Identifier (UPI), enacted by the Health Insurance Portability and Accountability Act of 1996 has been stalled by a Congressional prohibition on funding. However, the health information technology industry and other proponents are now trying to repeal the prohibition and advance a national patient identification system using other means.

Most citizens are unaware of federal plans for a national patient ID and a national computerized medical records system. The public continues to strongly support patient privacy and remains concerned about the impact of online electronic medical records on patient privacy and patient control over the sensitive personal details of their private lives. Policymakers should begin now to protect and restore patient privacy, patient trust, and patient data ownership rights by repealing the national patient ID and prohibiting its use.

** Twila Brase, RN, PHN, is president and co-founder of Citizens' Council for Health Freedom. CCHF exists to support patient and doctor freedom, medical innovation and the right of citizens to a confidential patient-doctor relationship.*

Endnotes

[1] Section 262 (Sec 1173), Title II, Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), August 21, 1996.

[2] Address on Health Care Reform (September 22, 1993), Bill Clinton, Miller Center, accessed December 23, 2011.

[3] "National Provider Identifier Standard," Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services, accessed December 7, 2011.

[4] "HIPAA Security 101," HIPAA Security Series, U.S. Department of Health and Human Services, March 2007, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf, accessed January 3, 2012.

[5] "MGMA Administrative Simplification Initiatives: Promulgation of the National Health Plan Identifier Regulations," Medical Group Management Association, n.d., accessed December 7, 2011.

[6] "Current CMS Regulatory Implementation Dates," HIPAA, Management Systems Consulting, http://msc-inc.net/documents/hipaa.html, accessed December 30, 2011.

[7] Section 262, Title II, Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191), August 21, 1996.

[8] "Patient Identity Integrity," HIMSS Patient Identity Integrity Work Group, Healthcare Information Management Systems Society, December 2009 (included in "Report to The Legislative Committee on Health Care, Senate Bill 319, Section 22, Unique Patient Identification Mechanism," Nevada State Health Division, July 1, 2010). http://health.nv.gov/HCQC/TechnicalBulletins/SB319_Sec22_Report_LCHC_Final_wLetter.pdf, accessed December 23, 2011.

[9] "Hearing Minutes," National Committee on Vital and Health Statistics, Subcommittee on Standards and Security, Chicago, Illinois, July 20-21, 1998, http://ncvhs.hhs.gov/980720mn.htm, accessed December 23, 2011.

[10] Section 516, Title V, Omnibus Consolidated and Emergency Supplemental Appropriations for FY 1999, H.R. 4328 (P.L. 105-277), October 21, 1998.

[11] "National Patient ID: Could a Voluntary System Fill the Gap?" Anne Paxton, CAP TODAY (College of American Pathologists), November 2009, http://bit.ly/Lix5O2, accessed December 23, 2011.

[12] Ibid.

[13] "Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System," by Richard Hillestad, James H. Bigelow, Basit Chaudhry, Paul Dreyer, Michael D. Greenberg, Robin C. Meili, M. Susan Ridgely, Jeff Rothenberg, and Roger Taylor, RAND Corporation, 2008, p. iii, http://www.rand.org/pubs/monographs/2008/RAND_MG753.pdf, accessed August 5, 2011.

[14] "Zambia Leads the Way in SmartCare Electronic Health Records System, a Benefit to Both Providers and Patients," George Muyunda, Jhpiego Corporation (an affiliate of Johns Hopkins University), n.d. http://www.jhpiego.org/en/content/zambia-leads-way-smartcare-electronic-health-records-system-benefit-both-providers-and-patie, accessed January 3, 2012.

[15] Ibid.

[16] Ibid.

[17] "SmartCare—One of the Largest Nationwide Electronic Medical Record System in Africa," Dimagi website, http://www.dimagi.com/smartcare/, accessed January 3, 2012.

[18] Ibid.

[19] Ibid..

[20] Ibid.

[21] Dimagi website, http://www.dimagi.com/about, accessed January 3, 2012.

[22] "SmartCare—One of the Largest Nationwide Electronic Medical Record System in Africa," Dimagi website, http://www.dimagi.com/smartcare/, accessed January 3, 2012.

[23] Muyunda, *op. cit*.

[24] "Report to The Legislative Committee on Health Care, Senate Bill 319, Section 22, Unique Patient Identification Mechanism," Nevada State Health Division, July 1, 2010.

[25] "Topic: Assembly Bill 280" (2011 Legislative Session), Nevada State Health Division Technical Bulletin, August 2011, http://health.nv.gov/HCQC/2011Bills/TechnicalBulletin_AB280.pdf, accessed December 23, 2011.

[26] Chapter 625 – S.F. No. 2192, Minnesota Legislature, 1994, Regular Session, https://www.revisor.leg.state.mn.us/laws/?doctype=Chapter&year=1994&type=0&id=625, accessed December 23, 2011.

[27] Minnesota Statutes 62J.54, 2000.

[28] "Using Social Security Numbers as identification numbers on Medicare cards" (Social Security Online FAQs), Social Security Administration, March, 2, 2012, http://1.usa.gov/KlAv6v, accessed June 12, 2012.

[29] "Against Simple Universal Health-Care Identifiers," Peter Szolovits and Isacc Kohane, Journal of the American Medical Informatics Association, 1994.

[30] "G98-1368 Medical Record Privacy" (Paper 388), Mary Ellen Rider et. al., University of Nebraska - Lincoln, 1998.

[31] Paxton, *op. cit.*

[32] "Part Three: Unique Patient Identifier," National Committee on Vital Health Statistics, U.S. Department of Health and Human Services, nd. http://ncvhs.hhs.gov/app3.htm, accessed December 5, 2011.

[33] "Public Attitudes Toward Medical Privacy," The Gallup Organization for Institute for Health Freedom, September 2000.

[34] Ibid.

[35] "Privacy and EHR Systems: Can We Avoid A Looming Conflict?" Dr. Alan F. Westin, (PPT presentation, Markle Conference on "Connecting Americans to Their Health Care," Washington, D.C.) December 7-8, 2006.

[36] Ibid.

[37] Telephone calls to author.

[38] "Proposed Changes to Privacy Rule Won't Ensure Privacy," Health Freedom Watch, Institute for Health Freedom, September 2010.

[39] "Universal Health Identifier: Invasion of Privacy or Medical Advancement?" Betty M. Ng, Rutgers Computer & Technology Law Journal, March 22, 2000.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] "Part Three: Unique Patient Identifier," National Committee on Vital Health Statistics, U.S. Department of Health and Human Services, nd. http://ncvhs.hhs.gov/app3.htm, accessed December 5, 2011.

[44] Ibid.

[45] "National Identification Cards: Legal Issues," Alison M. Smith, CRS Report for Congress, updated January 7, 2003.

[46] HHS notes that "All HIPAA covered entities would be affected by this interim final rule with comment period, as well as software vendors and any other business associates providing transaction related services, such as billing support and third party administrators (TPAs). Covered entities include all health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with a transaction for which the Secretary has adopted a standard. We note that health care providers may choose not to conduct transactions electronically. Therefore, they would be required to use these operating rules only for HIPAA transactions that they conduct electronically …. We assume that most providers and health plans use some electronic transactions and very few if any use none." Source: "Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transactions," Federal Register, Vol. 76, No. 131, July 8, 2011, p. 40477-78, http://www.gpo.gov/fdsys/pkg/FR-2011-07-08/html/2011-16834.htm, accessed December 23, 2011.

[47] "Administrative Simplification: Adoption of Operating Rules for Eligibility for a Health Plan and Health Care Claim Status Transactions," Federal Register, Vol. 76, No. 131, July 8, 2011, p. 40461, http://www.gpo.gov/fdsys/pkg/FR-2011-07-08/html/2011-16834.htm, accessed December 23, 2011.

[48] "The Development and Evolution of Operating Rules for Eligibility and Claims Status: A Key Component of Administrative Simplification as Mandated by the Patient Protection and Affordable Care Act of 2010," Council for Affordable Quality Healthcare Testimony to U.S. Department of Health & Human Services National Committee on Vital and Health Statistics Subcommittee on Standards, July 20, 2010, p. 26, http://www.caqh.org/pdf/CORE_NCVHSTestimony072010.pdf, accessed August 2, 2011.

[49] "Using the Nationwide Health Information Network to Deliver Value to Disability Claimants: A Case Study of Social Security Administration and MedVirginia Use of MEGAHIT for Disability Determination," by Sue S. Feldman, RN, MEd and Thomas A. Horan, PhD, Kay Center for E-Health Research, Claremont Graduate University, 2010, p. 7, http://www.medvirginia.com/includes/20100111_MedVA+Case+Study.pdf, accessed August 2, 2011.

[50] "The Importance of Standardized Health ID Cards for the National Health Information Network," by Patty Enrado, NHINWatch.com, December 7, 2006, http://www.nhinwatch.com/perspective/importance-standardized-health-id-cards-national-health-information-network, accessed August 2, 2011.

[51] "Group Pushes for Machine-Readable ID Cards," by Erik L. Goldman, FamilyPracticeNews.com, January 2010, http://fpn.imng.com/fileadmin/content_pdf/fpn/archive_pdf/vol40iss1/70090_main.pdf, accessed August 2, 2011.

[52] "Swiping Savings: MGMA Renews Push for Machine-Readable Insurance Cards, Estimating Savings Will Top $1 Billion," by Andis Robeznieks, ModernHealthCare.com, January 12, 2009, http://www.modernhealthcare.com/article/20090112/SUB/901099993, accessed July 22, 2011.

[53] "Health Identification Card Implementation Guide," Workgroup for Electronic Data Interchange, February 16, 2011, pp. 5, 7 and 39, http://www.ncpdp.org/EventFiles/021611%20WEDI%20Health%20ID%20Card%20Approved%20Ver%201-1%202-16-2011(2).pdf, accessed August 2, 2011.

[54] Ibid.

[55] "Group Pushes for Machine-Readable ID Cards," by Erik L. Goldman, FamilyPracticeNews.com, January 2010, http://fpn.imng.com/fileadmin/content_pdf/fpn/archive_pdf/vol40iss1/70090_main.pdf, accessed August 2, 2011.

[56] "Exhibit A: Unique Health Plan Identifier (HPID) WEDI Recommendations," Letter to The Honorable Kathleen Sebelius (RE: Unique Health Plan Identifier (HPID) Impact on Health Identification Cards), WEDI, January 14, 2011.

[57] "Patient Protection and Affordable Care Act; Standards Related to Reinsurance, Risk Corridors and Risk Adjustment; Proposed Rule," Federal Register, U.S. Department of Health and Human Services, July 15, 2011.

[58] "Patient Protection and Affordable Care Act; Standards Related to Reinsurance, Risk Corridors and Risk Adjustment" (Final Rule), 45 CFR Part 153, U.S. Department of Health and Human Services, Federal Register (Vol. 77, No. 57), March 23, 2012.

[59] Ibid.

[60] "Harnessing Health Information in Real Time: Back to the Future for a More Practical and Effective Infrastructure," Stephen T. Parente, American Enterprise Institute, December 8, 2010.

[61] Ibid.

[62] "Health IT Groups Urge Congress to Move on Unique Patient ID Solution," Kendra Casey Plank, BNA's Health IT Law & Industry Report, October 24, 2011.

[63] "Administrative Simplification: Adoption of a Standard for a Unique Health Plan Identifier; Addition to the National Provider Identifier Requirements; and a Change to the Compliance Date for ICD-10-CM and ICD-10-PCS Medical Data Code Sets," Proposed Rule, Office of the Secretary, Department of Health and Human Services, April 17, 2012.

[64] "RE: Unique Health Plan Identifier (HPID) Impact on Health Identification Cards," Letter to The Honorable Kathleen Sebelius, WEDI, January 14, 2011.

[65] 2009 IRS Form 990 for Council for Affordable Quality Healthcare, Inc.

[66] "The Development and Evolution of Operating Rules for Eligibility and Claims Status: A Key Component of Administrative Simplification as Mandated by the Patient Protection and Affordable Care Act of 2010," Council for Affordable Quality Healthcare Testimony to U.S. Department of Health & Human Services National Committee on Vital and Health Statistics Subcommittee on Standards, July 20, 2010, p. 3, http://www.caqh.org/pdf/CORE_NCVHSTestimony072010.pdf, accessed August 2, 2011.

[67] "Recommendations Regarding Sensitive Health Information," National Committee on Vital and Health Statistics (NCVHS) Recommendations to HHS, November 10, 2010, p. 1, http://www.ncvhs.hhs.gov/101110lt.pdf, accessed August 3, 2011.

[68] "Maintenance and Modifications for Standards and Operating Rules: Overview of Current Process for Operating Rules," testimony of Gwendolyn Lohse provided to the Subcommittee on Standards, National Committee on Vital and Health Statistics, April 27, 2011, CAQH, pp. 3, http://www.caqh.org/Reform/CORE_NCVHS042711ModTestimony.pdf, accessed August 2, 2011.

[69] "Phase III CORE Health Insurance Identification Card Rule Certification/Testing Subgroup Draft, March 23, 2010," Committee on Operating Rules for Information Exchange (CORE), March 23, 2010, p. 4, http://www.caqh.org/Host/CORE/Draft_PhaseIIIHealthIDCardRule03-23-10.pdf, accessed August 2, 2011.

[70] "MGMA Administrative Simplification Initiatives: Promulgation of the National Health Plan Identifier Regulations," Medical Group Management Association. n.d., accessed December 7, 2011.

[71] Committee on Operating Rules for Information Exchange (CORE), *op. cit.* March 23, 2010, p. 6.

[72] "CORE Phase I Eligibility and Benefits Operating Rules Manual," Committee on Operating Rules for Information Exchange (CAQH Initiative), April 2006.

[73] *Author's Note:* The name of the national health surveillance system has evolved from "National Health Information Infrastructure" to "National Health Information Network" to "Nationwide Health Information Network." We first noticed the switch from "National" to "Nationwide" in the 2005 report issued by the agency which noted that approximately 50% of the public comments on a request for information related to the NHIN were opposed to the NHIN. See: "Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses," U.S. Department of Health and Human Services, June 2005, http://www.cap.org/apps/docs/snomed/documents/0605_NHIN_rfisummaryreport.pdf, accessed June 8, 2012. The Department's switch of acronyms from NHIN to NwHIN came later. CCHF continues use of the pronounceable NHIN acronym for ease of communication with the public.

[74] CAQH [Gwendolyn Lohse testimony], *op. cit.* p. 21.

[75] "National Patient ID: Could a Voluntary System Fill the Gap?" Anne Paxton, CAP TODAY (College of American Pathologists), November 2009, http://bit.ly/Lix5O2, accessed December 23, 2011.

[76] Ibid.

[77] "Enterprise Master Patient Index," Wikipedia, http://en.wikipedia.org/wiki/Enterprise_Master_Patient_Index, accessed December 23, 2011.

[78] Paxton, *op.cit.*

[79] "Fundamentals for Building a Master Patient Index/Enterprise Master Patient Index (Updated)," Journal of AHIMA (updated September 2010), http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048389.hcsp?dDocName=bok1_048389, accessed December 23, 2011, (referencing "Masters of Their Domain," Robbi Hess, For The Record, August 15, 2005, http://www.fortherecordmag.com/archives/ftr_081505p30.shtml).

[80] "BocaArrowVideo VUHID 2011 09 09, YouTube, uploaded September 6, 2011 by openhealthtools, http://www.youtube.com/watch?v=kwvq1kKzKK4, accessed December 23, 2011.

[81] National Committee on Vital and Health Statistics, *op. cit.* July 20 - 21, 1998.

[82] Paxton, *op.cit.*

[83] Paxton, *op.cit.*

[84] "BocaArrowVideo VUHID 2011 09 09, *op. cit.*

[85] "Doctor-Patient Relationship: A Covenant of Trust," Singapore Medical Journal, 2001 Vol. 42(12): 579-581, http://www.sma.org.sg/smj/4212/4212sf3.pdf, accessed January 5, 2012.

[86] "Medical Privacy and Confidentiality Survey Summary and Overview," California HealthCare Foundation, January 28, 1999.

[87] "Standards for Privacy of Individually Identifiable Health Information," (Final Rule), Federal Register, Vol. 65, No. 250, Office of the Assistant Secretary for Planning and Evaluation, DHHS, December 28, 2000, pp. 82777 - 82779.