The Affordable Care Act Destroys Privacy

Twila Brase, R.N., P.H.N.

The Affordable Care Act (ACA or "ObamaCare") violates citizens' privacy. It uses federal laws designed by statists in order to impose control over medical practices.

Privacy-destroying laws include the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), which was enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA or the "Stimulus" bill). But the assault on privacy actually began with enactment of Medicare in 1965. Medicare payment proves the adage that he who holds the gold makes the rules. Since government is the Medicare payer, it was inevitable that its rules would soon include access to private patient data. Data equals control. For example, if Vermont Governor Shumlin has his way, Vermont will

> be the first state that moves to a system where we reimburse our providers for keeping us healthy. And that will change the whole economics of health care in Vermont, where docs, nurses, providers, and all of us as Vermonters will get financial rewards when we get off the smokes, eat right, exercise, do preventative care, do the mammogram, get folks in early and pay for it right up front so that anyone can access a doctor any time for health care needs to avoid the catastrophic care at the end.[1]

He calls these "patient-based payments." But they sound more like Pavlov-based payments using data gathered through medical record surveillance. In other words, if doctors and patients follow government-approved procedural and behavioral protocols, they'll be rewarded. Shumlin says Vermont will use the millions of dollars they've received in federal grants for health insurance exchange technology to develop this kind of payment system for the single-payer system Vermont is building.

History helps to explain how government achieved access to our private records.

HIPAA

Passed in 1996, HIPAA includes a section entitled "Administrative Simplification,"[2] which among other things requires medical identification and tracking numbers for patients, doctors, insurers, hospitals, clinics, and employers. Until his retirement, Rep. Ron Paul (R-Texas) effectively prohibited all federal funding for implementation of a national patient ID, officially called a Unique Patient Identifier (UPI). However, new federal rules and standardized operations under ACA may be an end-run around the prohibition.[3]

The 1996 law enabled medical data to be computerized without patient consent. It also required a medical privacy law to be enacted by Congress within three years, or alternatively written by the U.S. Department of Health and Human Services (HHS) if Congress failed to protect patients from the indiscriminate dispersal of private records made possible by electronic medical records and national data standards. Congress made a cursory attempt—enough to make Americans believe it meant to do something—and then handed the job of "protecting privacy" to HHS regulators. Congressmen probably didn't want to act—since lax privacy standards benefited some of their largest donors. Nor did any one of them want to be held personally responsible for the attack on patient privacy they had voted to implement under HIPAA.

The regulators didn't have the same political limitations.

A proposed "HIPAA Privacy Rule" was published on Nov 3, 1999,[4] as people were focused on their holiday celebrations. It made all sorts of deceitful comforting statements about the age-old right of patient privacy, but then proceeded to eliminate the need for patient consent for broad sharing of private medical records, including the sharing of private medical data with the government for 12 "national priority purposes." In an unprecedented outpouring of public angst, more than 52,000 public comments were sent to HHS, the majority of which opposed the denial of patient consent.

The Clinton Administration partially retreated, requiring patient consent for payment, treatment, and "health care operations," a term with a description more than 300 words long. This protection was insufficient, but it demonstrated a certain fear of the general public's anger. The consent requirement didn't last long. In March 2002, after President George W. Bush took office, the health insurance industry and other supporters of access to our confidential records convinced him to reconsider the final rule.

In the process, consent requirements extracted from the Clinton Administration were stripped away and additional outside access was given to something called a "limited data set" (LDS). For the specific purposes of "important research, public health and health care operations activities," the final HIPAA rule, published Aug 14, 2002, allowed government health officials, researchers, and others to have access to the full complement of a patient's data, as long as 18 data elements[5] were stripped out. The list was later cut down to 16 data elements. The prohibitions on "any other unique identifying number, characteristic or code" and on "all elements of dates," such as birth dates and admission and discharge dates, was eliminated.

One research group calls the LDS "a middle option that allows the use and disclosure of select identifiers with only limited Privacy Rule requirements."[6]

Partners Human Research Committee describes a limited data set as "personal health information that excludes the following direct identifiers of an individual or of relatives, employers or household members of the individual"[6] (see Table 1).

Table 1. Identifiers Stripped from Limited Data Set[6]

1. Names
2. Postal address information (e.g., street address, but town, city, state, ZIP code, and other geographic identifiers are permitted)
3. Telephone numbers
4. FAX numbers
5. Electronic mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plates
12. Device identifiers and serial numbers
13. Web universal resource locators (URLs)
14. Internet protocol (IP) address
15. Biometric identifiers, including finger and voice prints
16. Full-face photos and comparable images.

Partners also reports that Limited Data Sets can include the following identifiers:

1. Geographic data: A limited data set can include town, city, state and ZIP code, but no street address.

2. Dates: A limited data set can include dates relating to an individual (e.g., birth date, admission and discharge date).

3. Other unique identifiers: "A limited data set can include any unique identifying number, characteristic, or code other than those specified in the list of 16 identifiers that are expressly disallowed." [6]

Elimination of these 18 data elements, now 16, does not protect privacy. In fact, as HHS states in its final, Aug 14, 2002, rule regarding the original list of 18 elements, "We agree with those commenters who stated that the limited data set is not deidentified information, as retention of geographical and date identifiers measurably increases the risk of identification of the individual through matching of data with other public (or private) data sets." Instead, HHS vacuously requires "limitations on the specific uses" and deceptively states that requirements for the "data use agreement will provide sufficient protections for privacy and confidentiality of the data."

The revised HIPAA privacy rule became effective Apr 14, 2003. The rule gave at least 600,000 healthcare entities access to the patient's medical record without patient consent, ordered by HHS.[7] This number was later expanded to 701,325 entities.[8] Thus HIPAA is not a privacy law. It's a "NO-privacy" law.

HITECH

Then came HITECH in 2009. Sources differ, but HITECH gave at least $27 billion—some say up to $34 billion[9]—toward building a national medical records system. This system, long called the National Health Information Network (NHIN), was suddenly renamed the Nationwide Health Information Network (NwHIN) after the federal government received an array of negative public comments.[10] To further obscure its surveillance purposes, the network has again been renamed, and is now the eHealth Exchange.

The law also required use of interoperable electronic medical records by Jan 1, 2015. "Noncompliant" physicians and hospitals face Medicare reimbursement penalties. Although opinions differ about the term "interoperable," it essentially means computerized medical records that can communicate with other electronic data systems, allowing patient records to be disseminated broadly, not just to treating physicians and hospitals, but also to a host of entities now involved in the healthcare system, such as insurers and data aggregators.

However, simply owning and using such a patient record system was insufficient for regulators. Thus, the law requires "meaningful use" of the electronic medical record (EMR). Only those who comply with a myriad of "meaningful use" requirements are eligible to receive federal "incentive grants" to help cover a portion of the high cost of purchasing and setting up EMRs. "Meaningful use" essentially means that a doctor must use the EMR the way the government wants it used, which includes collecting and reporting certain patient data to the federal government for tracking and performance scoring.

Physicians may want to reconsider implementing the EMR. HHS is now employing a crew of auditors to check for approved use of "meaningful use" grants. Anyone who accepted those dollars may be forced to repay the entire grant if the federal auditors find any errors.[11]

HITECH also gave 1.5 million "business associates" access to private patient medical records without patient consent. Business associates are entities that perform "HIPAA-defined administrative and operational functions on behalf of the [HIPAA-covered entity such as doctors, hospitals and health plans] involving protected health information."[12] According to a July 2010 HHS regulation, HIPAA and HITECH together give more than 2.2 million entities access to patient data without patient consent.[13]

The Electronic Medical Record (EMR)

There is plenty to dislike about the EMR. For example, using an EMR "subjugates healthcare providers to increased regulation and scrutiny under the HITECH Act."[14] And as many doctors and nurses know, the EMR makes the practice of medicine and the care of patients more complicated and time-consuming, with data scattered on various screens. The EMR has been called "clunky, frustrating, user-unfriendly and inefficient."[15] In addition, patient histories and rationale for treatment decisions are often missing, leaving everyone in the dark.[16]

In other words, the exact reason for having an EMR is now ignored. A study found that medical students spend only 12 percent of their time with patients and 40 percent of their time with computers.[17] The EMR was built for billing, data collection, and government reporting requirements—not for taking care of patients.

But there are other serious concerns. For example:

- The director of the FDA's Center for Devices and Radiological Health testified that there have been at least six deaths and more than 40 injuries due to the EMR. He said this is probably the "tip of the iceberg."[18]
- Twenty-two types of medication error risks have been found due to Computerized Physician Order Entry.[19]
- One study found an increase in pediatric mortality.[20]
- Some EHR systems have crashed, leaving doctors and nurses without data.[21]
- The EMR gives government, health plans and health care systems control over medical practice. As one doctor told me, "If it's not on the computer screen, I can't do it."

Now comes the ICD-10, the new government-mandated system of diagnostic codes. Today, there are approximately 18,000 codes. Starting Oct. 1, 2014, there will be approximately 140,000 codes.[22] Government and health plan tracking of patients will be at a level of detail not previously possible. For example, the codes will record in what room of your house you were injured, and whether this is the first time you walked into a lamp stand or the second or third time. There are nine different codes for injuries from a macaw. If you were injured by a knitting or crochet needle, the government will know.

ACA Surveillance-Based Controls

ObamaCare is a data miner's dream. The surveillance and reporting provisions set in place the tools needed to impose a national healthcare system. I like to say, "He who holds the data makes the rules." A tyrant who does not track his subjects is a tyrant who can be undone. The federal government needs the information in our medical records to impose control over our doctors and our personal lives. A few examples of ObamaCare surveillance, which are included in our brochure called "Privacy and Health Care Reform,"[23] include but are not limited to:

1. IRS insurance status reporting and tracking;
2. Reporting medical data on all patients discharged from a hospital;
3. Prevention and wellness tracking programs;
4. Free drug sample tracking;
5. Annual Medicare "wellness visits" (I call them "inspections");
6. National Strategy to Improve Health Care Quality;
7. Home surveillance through $1.5 billion for home-visiting programs;
8. "Elder Justice," a program to track clinical care in long-term care facilities;
9. Fingerprinting and background checks for physicians;
10. "Health disparity" tracking and reporting; and
11. Health plan reporting of detailed patient data to the government.

The impact of government health surveillance should not be understated. One section of the law, Section 1311(h), allows the Secretary of Health and Human Services (HHS) to prohibit every insurer in the country from contracting with a physician if HHS determines the doctor does not provide "quality" healthcare as determined by the Secretary. Rep. Phil Gingrey (R-Ga.), a physician, has a bill to repeal the section. His bill is the SCOPE Act (Safeguarding Care Of Patients Everywhere).[24]

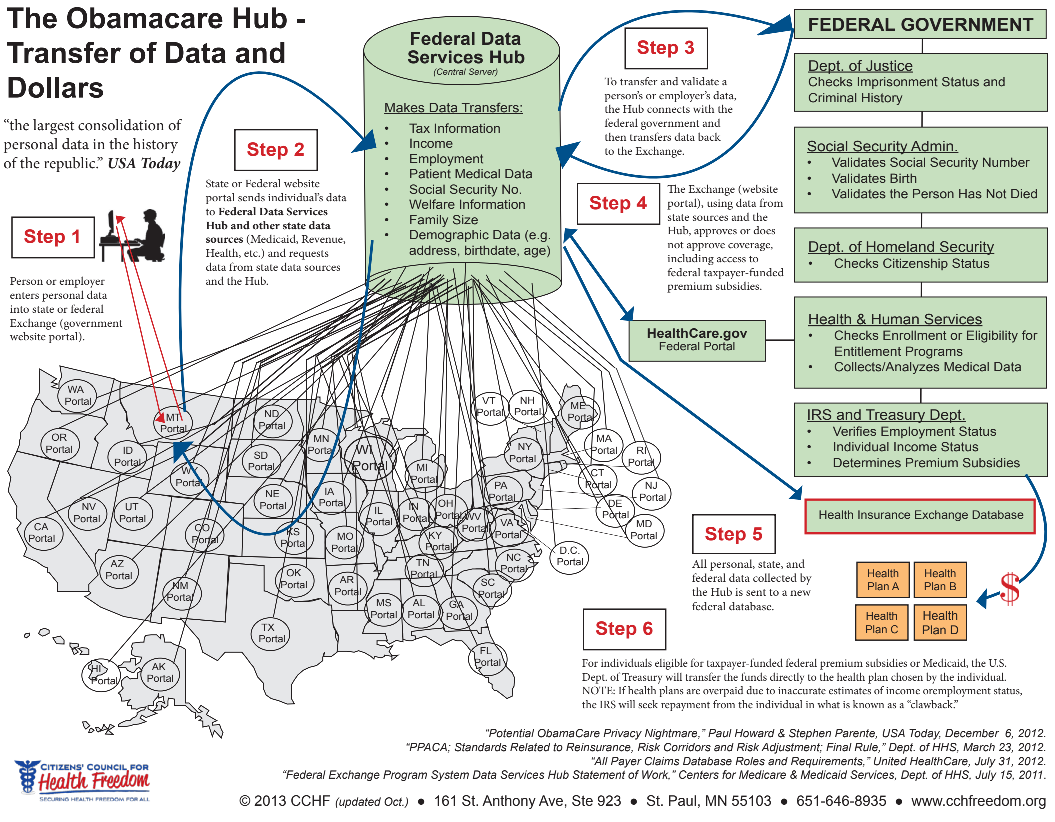
In addition, ACA provides $1.1 billion[25] for "comparative-effectiveness" research (CER) by the "Patient-Centered Outcomes Research Institute" (PCORI), formerly called the Federal Coordinating Council for Comparative Effectiveness Research—until the term became controversial. Using our tax dollars, this ACA agency is expected to produce research on how to ration medical care. PCORI will use data from patient medical records, purportedly with consent. But PCORI supporters have proposed that the consent process be less than forthright lest the patients become frightened by the thought of becoming research subjects.[26] They also propose that the data collection process for research be embedded within the medical record system to make data transfer easy—and hidden.[27]

PCORI's research will be used by the Secretary of HHS to determine "minimum essential benefits" for all insurance policies. Research "findings" will also impact decisions made by the ACA's Independent Payment Advisory Board (IPAB) regarding which medical treatments and procedures will or will not be reimbursed.

IPAB determinations are allowed by law to bypass the Congress and the President.[28] HHS can implement them immediately, unless Congress defeats them by a super-majority vote. Such votes are rare, so the IPAB will put patients' lives in jeopardy because 15 unelected, presidentially appointed, unaccountable IPAB bureaucrats can deprive every patient of medical treatment. Furthermore, ACA forbids Congress from repealing IPAB except during seven months in 2017, and even then requires a three-fifths vote from both chambers. Thus, the law unconstitutionally limits the power of Congress and creates an anti-constitutional "Super Legislature."[28]

The "ObamaCare Marketplace"

The master control and the largest surveillance system of all is ACA's Exchange, now euphemistically called "The Marketplace." It's important to understand that there is actually only one exchange. The national exchange system is made up of one central server—the Federal Data Services Hub (see Figure 1); 51 dummy terminals ("state exchanges"); a



The Obamacare Hub - Transfer of Data and Dollars

"the largest consolidation of personal data in the history of the republic." *USA Today*

Step 1: Person or employer enters personal data into state or federal Exchange (government website portal).

Step 2: State or Federal website portal sends individual's data to **Federal Data Services Hub and other state data sources** (Medicaid, Revenue, Health, etc.) and requests data from state data sources and the Hub.

Step 3: To transfer and validate a person's or employer's data, the Hub connects with the federal government and then transfers data back to the Exchange.

Step 4: The Exchange (website portal), using data from state sources and the Hub, approves or does not approve coverage, including access to federal taxpayer-funded premium subsidies.

Step 5: All personal, state, and federal data collected by the Hub is sent to a new federal database.

Step 6: For individuals eligible for taxpayer-funded federal premium subsidies or Medicaid, the U.S. Dept. of Treasury will transfer the funds directly to the health plan chosen by the individual. NOTE: If health plans are overpaid due to inaccurate estimates of income oremployment status, the IRS will seek repayment from the individual in what is known as a "clawback."

"Potential ObamaCare Privacy Nightmare," Paul Howard & Stephen Parente, USA Today, December 6, 2012.
"PPACA; Standards Related to Reinsurance, Risk Corridors and Risk Adjustment; Final Rule," Dept. of HHS, March 23, 2012.
"All Payer Claims Database Roles and Requirements," United HealthCare, July 31, 2012.
"Federal Exchange Program System Data Services Hub Statement of Work," Centers for Medicare & Medicaid Services, Dept. of HHS, July 15, 2011.

CITIZENS' COUNCIL FOR Health Freedom SECURING HEALTH FREEDOM FOR ALL

© 2013 CCHF *(updated Oct.)* • 161 St. Anthony Ave, Ste 923 • St. Paul, MN 55103 • 651-646-8935 • www.cchfreedom.org

Figure 1. Federal Data Services Hub and Its Connections

nationwide computerized network to connect the Hub to the dummy terminals, state agencies, and federal agencies; "state exchange" governance boards; and a new federal database to collect information gathered on all individuals having anything to do with the Exchange. This includes enrollees, potential enrollees, insurance agents, employers, Navigators, staff, and contractors. There are nine broad "routine uses" for which the data can be accessed without consent of the individual.

I have several names for the national exchange system, all descriptive of its many functions:

- Federal Takeover Center;
- ObamaCare Implementation Center;
- IRS Enforcement Center;
- National Insurance Status Tracking Center;
- Wealth Redistribution Center; and
- ObamaCare Funding Center.

President Obama's plan to have one central server and 51 dummy terminals hasn't gone as planned. Thirty-four states refused to cede control of healthcare to the federal government and consequently refused to fund and create a state dummy terminal into the system—and two agreed to do it but too late to make the Oct 1 deadline for open enrollment. This left the Obama Administration with no option but to create a federal dummy terminal called HealthCare.gov.

To be clear, the national exchange system has five components:

1. Dummy Terminals—Website portals run by states or HHS (*e.g. MNsure.org, coveredca.com, HealthCare.gov*);

2. Central Server—the Federal Data Services Hub, created by the federal government to collect data from individuals, state agencies, and federal agencies;[29]

3. IT infrastructure—a nationwide computerized network to connect the Hub, websites, health plans, and state and federal agencies for the purpose of data collection, insurance tracking, enforcement of the mandates, and transfer of tax dollars for ObamaCare premium subsidies;

4. Federal Database—a new "federal system of records" called the "Health Insurance Exchange Program" to collect and track the data collected by the Hub from individuals, states, and federal agencies;[30] and

5. State governance boards—located only in states that have funded their own dummy terminal and IT connections to the Hub ("state exchanges").

Data Collection

The standardized federal Exchange application for coverage currently only captures medical data elicited from the following three questions:

- Are you pregnant?
- If yes, how many babies are expected during this pregnancy?
- Do you have a physical, mental, or emotional health condition that causes limitations in activities (like bathing, dressing, daily chores, etc.) or live in a medical facility or nursing home?[31]

However, there are reasons to believe that the Exchange will eventually have broad access to patient medical records. First, the standardized design specifications for the Exchange websites—dummy terminals—were created by three federal agencies: the Centers for Medicare and Medicaid Services (CMS), the Center for Consumer Information and Insurance Oversight (CCIIO), and the Office of the National Coordinator for Health Information Technology (ONC)—an office tasked with creating a national medical record system called the eHealth Exchange.[32]

Second, state exchanges are charged with creating individual risk scores as part of the law's risk adjustment and re-insurance programs created to decrease the health plan's financial risk from individuals with pre-existing conditions.[33] If state exchanges choose not to calibrate the scores, the federal government can perform the task using patient data to build a risk profile of each health plan in the state. ACA created a $25 billion "Transitional Reinsurance Fund," which will compensate health plans that have the most high-risk patients enrolled.[34] A $63-per-head tax will be collected from insurers and placed in the fund beginning in 2014.[35] The 3-year tax, which will increase insurance premiums, decreases each year.

Third, the Exchanges must collect "quality data" on doctors and hospitals and make it available to enrollees for choosing between coverage options. This "quality" scorecard is created by using private data in patient medical records. The question of full data integration between Health Information Exchanges (HIE) and Health Insurance Exchanges (HIX) came up at the eHealth Initiative 2013: Health Data Exchange & Interoperability Summit that I attended Oct 31, 2013. One panelist said the portability of insurance will "bring these together at some point of time." But they "don't have the tools" to do it now.

What does "quality data" on the Exchange actually mean? Since outsiders—government and insurers—will define "quality," data provided to potential enrollees are compliance data. Thus, the worst doctors may look the best, while the best doctors—those who treat according to the individualized needs of patients—may look the worst. And regardless of what the scores mean, most Exchange patients will end up in "narrow network" plans with limited choice of doctors. Thus, regardless of the scores, there will be only so many doctors from which to choose.

Little Security of Exchange Data

With the national Exchange system creating "the largest consolidation of personal data in the history of the republic,"[36] is the data secure? Probably not. The Exchanges opened their doors on Oct 1, 2013, and few people could enter. Just six people were able to enroll on the first day.[37] The systems were overloaded, the connections to the Data Hub didn't work, and those who were actually interested in Exchange coverage were frustrated. Even news reporters couldn't get in. The media reported people trying day after day, sometimes for hours on end to enroll, without success.

If these were the "glitches" in enrollment, imagine the "glitches" in security. There are valid reasons for concern. The Inspector General of HHS (IG) reported in August 2013 that the security of the system could not be tested until Sept 30, 2013, at the earliest—one day before open enrollment. Then five days before the U.S. House held a hearing on the issue of Exchange and Data Hub security, HHS suddenly announced that the system was secure—three weeks before Sept. 30. Testifiers and members of Congress were not convinced.[38] The IG had not independently verified the security, and the IG had no plan to verify it.[39] She would accept HHS's self-attestation.

Other security problems also emerged. HHS acknowledged in testimony before Congress that ACA "Navigators," tasked with enrolling people in the Exchange, would not be subject to background checks and may have criminal histories. Several other testifiers said people enrolling on the exchange would be vulnerable to fraud, hackers, and identity theft. As one example of data security issues, an employee of MNsure, Minnesota's ACA exchange, released information on 2,400 insurance agents, including Social Security numbers, to an insurance broker, before the exchange was even operating.

Data security remained an issue even after the start of open enrollment. Three weeks later, a software tester discovered a simple way to hack into anyone's account.[40] Then on Oct 30, a security hole in the Spanish language version of healthcare.gov was discovered.[41]

On Oct. 15, 2013, two members of Congress sent a letter to HHS seeking answers on Data Hub security, asking for evidence of Hub certification and inquiring about the Exchange database created to store data on individuals despite hearing testimony that the Hub would not store data.[42]

Stopping the Intrusive Control

In the battle to stop ACA and the federal takeover of medicine, it's important to remember that he who holds the data makes the rules.

Patient data will be used to ration care and control physicians. IRS will use ACA's Exchange to police the individual and employer mandates and to impose the "uninsured tax" penalty on non-exempt individuals who refuse to purchase health insurance or accept government coverage. Seven hundred pages of the 2,700-page bill were a rewrite of the IRS code to empower the IRS with access to personal data.[43]

Doctors have an important role to play. To restore physician control over the practice of medicine, doctors should refuse to implement an EMR or, if they choose to use one solely for their own office, they should refuse to share or transmit any patient data outside clinic walls without specific and limited patient consent.

Doctors should sell privacy as a benefit available at their clinic. Patients of all political stripes prefer privacy. Many people desperately need it. Physicians can offer a clear choice to patients: a private record with no government or insurer access. Privacy is a selling feature. Physicians should market it; go cash-only to protect it; and educate patients with materials like the Citizens' Council for Health Freedom's "10 Things to Know" brochure[23] on privacy and health care reform.

Patients and physicians must work together to undo HIPAA's intrusions, protect patient privacy, and stop ACA until it is repealed and health freedom is secured.

The Citizens' Council for Health Freedom's motto concerning ACA is "Resist. Repeal. Reclaim." We can and we will reclaim health freedom. To do so, we must stop government intrusions into the medical record.

It can be done.

It must be done.

Twila Brase, R.N, P.H.N, is president and co-founder of Citizens' Council for Health Freedom. Contact: twila@cchfreedom.org.

REFERENCES

1. Central Vermont Television. City Room with Steve Pappas: with Gov. Peter Shumlin. Vimeo. Available at: http://vimeo.com/73801468. Accessed Nov 9, 2013.
2. Legal Information Institute. 42 USC Part C—Administrative Simplification. Cornell University Law School; n.d. Available at: http://www.law.cornell.edu/uscode/text/42/chapter-7/subchapter-XI/part-C. Accessed Nov 1, 2013.
3. Brase T. National patient ID. Policy Insights. Citizens' Council for Health Freedom, July 2012.
4. Office for Civil Rights, U.S. Department of Health and Human Services. Summary of the HIPAA Privacy Rule. OCR Privacy Brief, Last Revised May 2003. Available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf. Accessed Nov 1, 2013.
5. National Institutes of Health, Department of Health and Human Services. How can covered entities use and disclose protected health information for research and comply with the Privacy Rule? HIPAA Privacy Rule: Information for Researchers. Available at: http://privacyruleandresearch.nih.gov/pr_08.asp. Accessed Oct 5, 2013.
6. Partners Human Research Committee, Partners Healthcare. Limited Data Sets in Research. Available at: http://healthcare.partners.org/phsirb/limdata.htm. Accessed Oct 5, 2013..
7. Office for Civil Rights, U.S. Department of Health and Human Services. Standards for Privacy of Individually Identifiable Health Information. Final Rule; Request for Comments. RIN: 0991-AB08, 45 CFR Parts 160 and 164. Federal Register 2001; 66(40, Feb 28):12738-12739.
8. Modifications to the HIPAA Privacy, Security, and Enforcement Rules under the Health Information Technology for Economic and Clinical Health Act. RIN: 0991–AB57. Federal Register 2010;75(134, Jul 14):40907.
9. Citizens' Council for Health Freedom. Conservative think tank proposes real-time health risk score for all. *Health Freedom Watch*, November 2011. Available at: http://www.cchfreedom.org/newsletter.php/38. Accessed Nov 1, 2013.
10. Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. Summary of Nationwide Health Information Network (NHIN) Request for Information (RFI) Responses; June 2005. Available at: http://library.ahima.org/xpedio/groups/public/documents/government/bok1_027626.pdf. Accessed Nov 1, 2013.
11. Youngstrom N. CMS recoups all meaningful use money from providers if audits turn up errors. *AIS Health*, Sept 16, 2013. Available at: http://aishealth.com/archive/rmc090913-01. Accessed Nov 1, 2013.
12. Morris D. Final HIPAA amendments expand HIPAA net: business associates now required to enter into business associate agreements with subcontractors. Alerts and Updates, Jan 23, 2013. Available at: www.duanemorris.com/alerts/final_HIPAA_amendments_expand_HIPAA_net_4724.html. Accessed Nov 1, 2013.
13. Institute for Health Freedom. Proposed changes to privacy rule won't ensure privacy. *Health Freedom Watch*, September 2010. Available at: http://forhealthfreedom.org/Newsletter/September2010.html#Article3.

Accessed Nov 1, 2013.

14. Rhodes H. Meaningful Use program faces audits, scrutiny. *J AHIMA* 2013;84(2). Available at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050010.hcsp?dDocName=bok1_050010. Accessed Nov 1, 2013.
15. Soumerai S, Koppel R. A major glitch for digitized health-care records. *Wall St J*, Sept 17, 2012. Available at: http://online.wsj.com/news/articles/SB10000872396390443847404577627041964831020. Accessed Nov 1, 2013.
16. Dawson G. More talk on psychiatry and the Affordable Care Act. *Real Psychiatry Blog*, Jul 11, 2013.
17. Barclay L. Medical interns spend very little time at patient bedsides. *Medscape Medical News,* Apr 25, 2013.
18. Testimony of Jeffrey Shuren, Director of FDA's Center for Devices and Radiological Health to the Health Information Technology (HIT) Policy Committee Adoption/Certification Workgroup, Feb 25, 2010. Available at: http://www.cchfreedom.org/files/files/Health%20IT%20Deaths%20-%20FDA%20jeffrey%20Shuren.pdf. Accessed Oct 5, 2013.
19. Koppel R, Metlay JP, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. *JAMA* 2005;293:1197-1203. Available at: www.ncbi.nlm.nih.gov/pubmed/15755942. Accessed Nov 1, 2013.
20. Han YY, Carcillo JA, Venkataraman ST, et al. Unexpected increased mortality after implementation of a commercially sold computerized physician order entry system. *Pediatrics* 2005;116:1506-1512. Available at: http://pediatrics.aappublications.org/content/116/6/1506. Accessed Oct 5, 2013.
21. McCann E. Setback for Sutter after $1B EHR crashes. *Healthcare IT News*, Aug 28, 2013. Available at: www.healthcareitnews.com/news/setback-sutter-after-1b-ehr-system%20crashes. Accessed Oct 5, 2013.
22. Mathews AW. Walked into a lamppost? Hurt while crocheting? Help is on the way. *Wall St J*, Sept 13, 2011.
23. Citizens' Council for Health Freedom. *Privacy and Health Care Reform: Ten Things Patients and Doctors Need to Know*. Available at: www.cchfreedom.org/cchf.php/206. Accessed Oct 5, 2013.
24. Gingrey P. SCOPE Act: protecting the physician-patient relationship. *National Review Online*, Oct 24, 2012. Available at: http://www.nationalreview.com/critical-condition/331574/scope-act-protecting-physician-patient-relationship-phil-gingrey. Accessed Oct 5, 2013.
25. U.S. Department of Health and Human Services. HHS names Federal Coordinating Council for Comparative Effectiveness Research. Press Release, Mar 19, 2009. Available at: www.hhs.gov/news/press/2009pres/03/20090319a.html. Accessed Oct 5, 2013.
26. Patient-Centered Outcomes Research Institute. Cooperative Agreement Funding Announcement: Improving Infrastructure for Conducting Patient-Centered Outcomes Research; Apr 23, 2013. Available at: http://www.pcori.org/assets/PCORI-CDRN-Funding-Announcement-042313.pdf. Accessed Nov 1, 2013.
27. Brase T. Watered-down patient consent? *CCHF Health Freedom eNews*, Sept 18, 2013. Available at http://healthenews.cchfreedom.org/newsletter.php/99. Accessed Nov 1, 2013.
28. Cohen D, Cannon MF. The Independent Payment Advisory Board: PPACA's anti-constitutional and authoritarian super-legislature. Policy Analysis No. 700, Cato Institute, Jun 14, 2012. Available at: www.cato.org/publications/policy-analysis/independent-payment-advisory-board-ppacas-anticonstitutional-authoritarian-superlegislature. Accessed Oct 5, 2013.
29. Centers for Medicare and Medicaid Services, Department of Health and Human Services. Federal Exchange Program System Data Services Hub Statement of Work. Draft, Version 1.0, Jul 15, 2011. Available at: www.cchfreedom.org/pdfs/HIX%20HHS%20-%20Hub%20Statement%20of%20Work%20RFP%20HIX%20Federal%20.pdf. Accessed Nov 1, 2013.
30. Centers for Medicare and Medicaid Services. Privacy Act of 1975: Notice to establish a new system of records. Federal Register 2013;78(25, Feb 6):8538-8542. Available at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-06/pdf/2013-02666.pdf. Accessed Nov 1, 2013.
31. Health Insurance Marketplace. Application for Health Coverage & Help Paying Costs (Short Form). OMB No. 0938-1191; no date. Available at: http://marketplace.cms.gov/getofficialresources/publications-and-articles/individual-short-form.pdf. Accessed Nov 1, 2013.
32. Citizens' Council for Health Freedom. *The Big Blue Book*. Available at: www.cchfreedom.org/cchf.php/657. Accessed Oct 5, 2013.

33 Department of Health and Human Services. Patient Protection and Affordable Care Act: Standards Related to Reinsurance, Risk Corridors and Risk Adjustment: Final Rule, 45 CFR Part 153. Federal Register 2012;77(57, Mar 23):17220-17252. Available at: www.gpo.gov/fdsys/pkg/FR-2012-03-23/pdf/2012-6594.pdf. Accessed Nov 1, 2013.

34 Brase T. New health fee for employers. *CCHF Health Freedom eNews*, Oct 23, 2013. Available at: http://healthenews.cchfreedom.org/newsletter.php/105. Accessed Nov 1, 2013.

35. U.S. Department of Health and Human Services. Patient Protection and Affordable Care Act; HHS Notice of Benefit and Payment Parameters for 2014 and Amendments to the HHS Notice of Benefit and Payment Parameters for 2014; Final Rules; Patient Protection and Affordable Care Act; Establishment of Exchanges and Qualified Health Plans; Small Business Health Options Program; Proposed Rule. Federal Register 2013;78(47, Mar 11):15410-15541. Available at: http://www.gpo.gov/fdsys/pkg/FR-2013-03-11/html/2013-04902.htm. Accessed Nov 1, 2013.
36. Parente ST, Howard P. Potential ObamaCare privacy nightmare. *USA Today*, Dec 6, 2012. Available at: http://www.usatoday.com/story/opinion/2012/12/06/column-potential-obamacare-privacy-nightmare/1752211/. Accessed Oct 5, 2013.
37. Roy A. The truth comes out: Obamacare's website enrolled a grand total of six people on October 1. *Forbes*, Nov 1, 2013. Available at: http://www.forbes.com/sites/theapothecary/2013/11/01/the-truth-comes-out-obamacares-website-enrolled-a-grand-total-of-six-people-on-oct-1/. Accessed Nov 1, 2013.
38. Sternstein A. Obamacare data hub security review blasted. *NextGov*, Sept 12, 2013. Available at: www.nextgov.com/cybersecurity/2013/09/obamacare-data-hub-security-review-blasted/70220/?oref=nextgov_today_nl. Accessed Nov 1, 2013.
39. Sternstein A. Health agency watchdog doesn't have time to vet Obamacare cyber designs. *NextGov*, Sept 16, 2013. Available at: www.nextgov.com/cybersecurity/2013/09/health-agency-watchdog-doesnt-have-time-vet-obamacare-cyber-designs/70352/?oref=ng-relatedstories. Accessed Nov 1, 2013.
40. Pagliery J. Security hole found in Obamacare website. *CNN Money*, Oct 29, 2013. Available at: http://money.cnn.com/2013/10/29/technology/obamacare-security/. Accessed Nov 1, 2013.
41. Sternstein A. Researchers find a way to hack Spanish language Healthcare.gov. *NextGov,* Oct 30, 2013. Available at: www.nextgov.com/cybersecurity/2013/10/researchers-find-way-hack-spanish-language-healthcaregov/72962/?oref=ng-relatedstories. Accessed Nov 1, 2013.
42. Black M. Seek answers on security of Obamacare data hub. Press Release, Oct 16, 2013. Available at: http://black.house.gov/press-release/black-meehan-seek-answers-security-obamacare-data-hub. Accessed Nov 1, 2013.
43. Citizens' Council for Health Freedom. Exchanges Called "lynchpin" of reform. *Health Freedom Watch*, March 2011. Available at: www.cchfreedom.org/newsletter.php/16. Accessed Nov 1, 2013.