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 statisticians 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,”⁵ 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 elements⁶ 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.”⁷ 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”⁸ (see Table 1).
medical records by Jan 1, 2015. “Noncompliant” physicians and
purposes, the network has again been renamed, and is now the
(NwHIN) after the federal government received an array of
suddenly renamed the Nationwide Health Information Network
called the National Health Information Network (NHIN), was
building a national medical records system. This system, long
awaited by HHS.

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 billion9—to build
a national medical records system. This system, long
called the National Health Information Network (NHN), 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 doctor who 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 “Patient-Centered Outcomes Research” (PCORI), formerly called the “Outcomes Research Institute.”24

In addition, ACA provides $1.1 billion25 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.”29

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...
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:
1. Federal Takeover Center;
2. ObamaCare Implementation Center;
3. IRS Enforcement Center;
4. National Insurance Status Tracking Center;
5. Health Redistricting Center; and
6. 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?²³

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,
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.

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 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


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