August 2013

POLICY INSIGHTS

Patient Privacy and Public Trust:

How Health Surveillance Systems Are Undermining Both

By Twila Brase

President, Citizens' Council for Health Freedom

Executive Summary

With significant funding from Congress, state health departments have created a multitude of government patient-tracking systems. Increasingly, these systems are being linked together, creating individual health profiles and lifelong records.

The emergence of computerized medical records—and the federal requirement that physicians, hospitals and other health care professionals have interoperable electronic medical records for data sharing or be penalized in 2015[1] —has accelerated and facilitated government access to private patient data. Usually without consent, private patient data is being collected from doctors, hospitals, and clinics – in some cases annually for lifelong monitoring.

The data is often entered into state registries, databases, or, in the case of newborn screening dried blood spots, state DNA biobanks. The number of disease and condition-specific state databases and registries is growing, but this report covers just four of the many government health surveillance systems:

- Birth defects surveillance systems
- Cancer registries
- Newborn screening databases
- Vaccination/Immunization registries

These four systems are found in all or almost all 50 states and the District of Columbia, and each one has received federal funding. Many still do. Most Americans are in at least one of these surveillance systems. For

Companion Charts:

- Table of raw data collected from state agencies in 50 states and D.C. on four or more health surveillance systems
- 50 state tables of statutory language for four different surveillance systems
- One 50-state table for each of four state surveillance systems
- 204 individual tables - one for each state surveillance system plus D.C.

The full report and all companion charts can be found at:
http://bit.ly/HealthSurveillanceReport

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

CITIZENS' COUNCIL FOR Health Freedom
SECURING HEALTH FREEDOM FOR ALL

example, children are in all four systems, although not all children are in all of them. Adults with cancer are in the cancer registry, and increasingly adults are in the vaccination registry. Furthermore, mothers are often registered in systems that register their children.

HIPAA: Protection or Permission Slip?

Most of the public believes the federal HIPAA "privacy" rule protects their privacy. However, HIPAA is a disclosure rule. The rule—required by the Health Insurance Portability and Accountability Act 2006 (HIPAA)—allows approximately 600,000 entities, including government agencies, to collect, store, use and share private patient data without the individual's consent for many reasons, including "public health purposes." In addition, the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, added 1.5 million business associates. Together, HIPAA and HITECH allow more than 2.2 million entities to access patient medical records data without patient consent. Although state health officials readily promise to protect the privacy of the data once it's collected, state departments are no longer protecting the individual's privacy. They are only promising to protect the security of the individual's data within the government system.

Significant Intrusion

The four surveillance systems discussed in this report are just a subset of the vast public health surveillance system. This report shows that health surveillance is a significant, intrusive and growing activity of state and federal government agencies. It demonstrates how government officials are collecting, analyzing, using, linking and sharing Americans' private health data without their knowledge or consent.

Threat to Patient Trust

Patient trust is critical to good medical care. Once the public becomes aware of the government's use of clinics, hospitals, physicians, and other practitioners to build state-based patient-tracking systems, collect DNA, and conduct health surveillance and research, the patient-doctor relationship and the patient trust necessary for frank conversations and timely access to care may be threatened. At least 15 percent of the public have already taken evasive action to protect their privacy including delaying medical care or refusing to seek medical attention, according to a 1999 California Healthcare Foundation study—and that was 14 years ago.

This Report

Our report is intended to inform the public about the virtually unknown state health surveillance systems that currently allow surreptitious government intrusion in patient lives in the name of "public health." The public which does not know cannot act. Once informed by our report, individuals may seek legislative action to require informed written consent or to limit the broad sharing and use of data permitted under HIPAA. They may also take other personal actions to protect their medical privacy and restore their privacy rights.

Endnote:

1 The HITECH ACT within the American Recovery and Reinvestment Act of 2009 ("economic stimulus") requires physicians, hospitals and other health care practitioners to use "interoperable electronic medical records" by 2015 in a "meaningful" way as defined by the federal government or face financial penalties through reduced Medicare payments, starting in 2015.