50-State Report Unveiled; States Track Medical Data from Birth to Death Without Consent

Eight Years of Research by CCHF Shows That States are Secretly Building Private Medical Registries to Tie into National Surveillance Networks

ST. PAUL, Minn.— Today, Citizens’ Council for Health Freedom (CCHF, CCHFreedom.org) is releasing the findings of one of its most important works to date. For the past eight years, CCHF has been researching health departments in all 50 states to find out how they use funding from the federal government to obtain and store citizens’ private medical information—in most cases, without patients’ consent.

CCHF’s report, “Patient Privacy and Public Trust: How Health Surveillance Systems Are Undermining Both,” includes details about all of the private patient data that states collect and maintain. One alarming fact, says patient advocate and co-founder of CCHF, Twila Brase, is that the information is stored and identified along with the name of each individual American.

“We have conducted over eight years of research and we’ve found that states are building health profiles of individuals starting from childhood,” Brase said. “These are long-term tracking systems without the person’s knowledge or choice. Private data is being analyzed, and if patients have the option to ‘opt out,’ they leave behind a record making them vulnerable to being stamped as ‘anti-government.’ What we found is a scary, disturbing intrusion into Americans’ privacy, and a violation of our Fourth Amendment rights, which protect us from unreasonable searches and seizures without probable cause—and that applies to our private medical information, too.”

For nearly a decade, Brase has researched the medical data that states collect on Americans—from birth to death—on everything from birth defects to cancer diagnoses. Brase’s report, released today, contains extensive information on the types of health data collected by states, including but not limited to: hospital discharge data, vaccination and newborn genetic screening data, cancer diagnosis and treatment data, as well as data on individuals diagnosed with ADHD, autism, birth defects, diabetes, asthma, sexually transmitted diseases, strokes and cardiovascular disease, Alzheimer’s disease, ER visits, obesity and injuries. Other personal information collected and stored includes the patient’s name, address, sex, race, ethnicity, date of birth, Social Security number and occupation.
Brase and her team at CCHF bring to light many findings in their groundbreaking work, including:

- States have created an array of government patient-tracking systems, and they are given government money to create and maintain these databases.
- As a part of the federal funding requirement, state agencies overseeing these systems share patient health information with various federal agencies, including the Centers for Disease Control and Prevention (CDC) and the Department of Health and Human Services (HHS).
- Federal requirements for computerized medical records, and the so-called federal HIPAA privacy rule, have facilitated government access to patient data.
- Patient consent for collection and use of their data is typically not required, although dissent is sometimes permitted.
- Government workers can enter hospitals and clinics to collect your data without your consent.
- **With no consent requirement, members of the public are probably not aware of the vast array of state surveillance systems or that they and their children could be entered into and named individually in one or more of the patient-tracking systems.**
- Funding for health surveillance systems comes from the federal government, state legislatures and private organizations. The data systems can be expensive to maintain. For example, electronic state immunization registries have been supported by at least $142 million in federal funds and more than $200 million in other funding, meaning that these registries can cost as much as $217 per child per year.
- To demonstrate the development and funding of state health surveillance systems, including data collection and use of private data, the report, with 51 online charts, focuses on four uniform data systems found in all or most of the 50 states and Washington, D.C.
- Patient trust, which is key to excellent medical care, may be harmed once patients understand their private data is shared with the government for health surveillance.
- State legislatures can restore patient consent and privacy rights.

“The way that our government gets a hold of our data is wrong. It’s a violation of our rights, pure and simple,” Brase said. “If you have a certain disease, the government gets that data without your consent. Get a trackable condition and you suddenly become the subject of a government surveillance system without your consent. These surveillance systems have been hidden from Americans, but once the public knows, they will be outraged—and they should be.”