Clinic Closes After Massive Hack—Just One of the Many Dangers of Electronic Health Records

_Citizens’ Council for Health Freedom_ Points to Pitfalls of EHRs in Award-Winning Book, ‘Big Brother in the Exam Room’

ST. PAUL, Minn.—A huge patient data hack at a Michigan clinic this spring caused two doctors to retire early and close their office for good.

This hack that crippled and killed an entire medical practice wasn’t the first, says _Citizens’ Council for Health Freedom (CCHF)_ and it won’t be the last.

Brookside ENT and Hearing in Michigan is permanently closed after a ransomware attack took control of its computerized medical records. The two doctors running the practice refused to pay a $6,500 ransom to retrieve the files, so hackers wiped out the entire computer system, and all patient data was deleted.

“Rather than rebuild their practice from scratch, the doctors retired early, leaving their patients to find care, and scheduled surgery elsewhere,” said CCHF president and co-founder Twila Brase. “When Congress mandated that doctors use electronic health records, it opened the door to hacking. This is just one of the many dangers electronic health records (EHRs) pose to patients, and nearly everyone’s private medical information has been entered into an EHR sometime in the course of their care, and therefore, is at risk.”

In her extensively researched and award-winning book, “_Big Brother in the Exam Room: The Dangerous Truth About Electronic Health Records_,” Brase exposes how the mandated, government-certified EHR technology (CEHRT) has negatively affected doctors and patients. “_Big Brother in the Exam Room_” also shows how and why Congress forced doctors and hospitals to install a data-collecting, command-and-control surveillance system in each exam room.

“The watched are never free,” Brase writes in “Big Brother in the Exam Room.” “Surveillance is and has always been a tool of control. That’s why America’s Founding Fathers put privacy protections in the U.S. Constitution, as part of the Bill of Rights. However, the emergence of new surveillance-enabled technologies today—such as computers, smartphones, digital driver’s licenses and biometric scans—create new tracking and analytic powers. Unless Americans remain watchful and engaged, their freedom can be taken away, one law and one technology at a time.”

More recently, an Ohio medical practice was allegedly hacked and told to pay $75,000 in ransom to unlock its computer system. According to _FierceHealthcare.com_, N.E.O. Urology Associates agreed to pay the ransom using bitcoin in order to access its computer system. But the hack so disrupted their system, it took two days to access the data. They estimate a loss of $30,000 to $50,000 in revenue per day. Police are investigating.
In 2018, the Indiana-based Hancock Health paid a $55,000 ransom to hackers to release more than 1,400 files and regain control of the clinical IT systems at Hancock Regional Hospital, FierceHealthcare also reported.

“Big Brother in the Exam Room” also includes the impact of EHRs on privacy, patient care, costs, patient safety and more, according to doctors and over 125 studies, as well as details the privacy-stealing HIPAA rule (Section IV), socialized medicine, patient privacy, health freedom and how the Affordable Care Act has harmed patients and doctors since 2010. Learn more at www.BigBrotherintheExamRoom.com.

Learn more about CCHF at www.cchfreedom.org, its Facebook page or its Twitter feed @CCHFreedom. Also view the media page for CCHF here. For more about CCHF’s initiative The Wedge of Health Freedom, visit www.JointheWedge.com, The Wedge Facebook page or follow The Wedge on Twitter @wedgeoffreedom.