Editorial:
MATRIX: Threat to Medical Privacy?

Lawrence R. Huntoon, M.D., Ph.D.

Medical privacy, the foundation of trust embodied in the patient-physician relationship, has been placed in great jeopardy.

On the heels of the Pentagon's publicly rebuked TIA program–Total Information Awareness–comes the latest acronym designed to satisfy government's insatiable appetite for more and better access to our individual information: MATRIX.

Developed by Seisint, Inc., MATRIX is the Multi-State Anti-Terrorism Information Exchange. The word "matrix" also derives from the Latin *mater*, or "mother." Information posted on the MATRIX website (http://www.matrix-at.org) reveals that it is indeed the mother of all government-controlled information systems.

According to information on the website, MATRIX is a "pilot effort to increase and enhance the exchange of sensitive terrorism and other criminal activity information between local, state and federal law enforcement agencies." It uses supercomputer technology with new data linking methods, with a networked computerized system known as RISS.net–Regional Information Sharing Systems–as its "communications backbone." Each of the participating states represents a node on RISS.net. Currently only eight states participate (Connecticut, Florida, Georgia, Michigan, New York, Pennsylvania, Ohio, and Utah), but the "ultimate goal is to expand this capability to all states."

FACTS: Factual Analysis Criminal Threat Solution–a part of MATRIX–essentially represents a sophisticated search engine that allows law enforcement to "access criminal, public and commercial databases." Seisint, the information management and technology company which developed the MATRIX system, "stores billions (at least 20 billion according to some accounts) of records that can be searched, analyzed, and compiled quickly," according to the MATRIX website.

The list of data available in MATRIX's reference repository reminds one of the teenager in the movie *American Graffiti*, who went into the convenience store and ordered a Three Musketeers candy bar, a ballpoint pen, a comb, a couple of flashlight batteries, some beef jerky, and oh, by the way, interspersed with the rest, a pint of Old Harper. Data available in the government's repository includes: "FAA pilot licenses and aircraft ownership, property ownership, Coast Guard registered vessels, state sexual offenders lists, federal terrorist watch lists, corporation filings, uniform commercial code filings, bankruptcy filings," and oh, by the way, "commercial sources are used where they are generally available to the public or *legally permissible under federal law*" [emphasis added].

Since the passage of the Health Insurance Portability and Accountability Act it is now "legally permissible under federal law" for law enforcement at all levels to access private, confidential medical records without a warrant or subpoena, for the purpose of oversight and compliance.

Andrew Schlafly, Esq., AAPS general counsel, has described the legal threshold for government requesting medical records as "nil" pursuant to its oversight authority for HIPAA-covered entities. Inquiries have been made to MATRIX officials regarding the accessibility of patient medical records, but other than simple referrals to the MATRIX website–which does not specifically address the issue–the question has gone unanswered.

Insurance companies have had access to a networked system, a commercial database, for sharing information on individual clients for many years. As access to this information is now "legally permissible under federal law," what will prevent law enforcement from using MATRIX to search this database?

Clearly, some think that government access to health information is crucial in the fight against terrorism. A recent report by the Markle Foundation, whose security task force includes retired general and former presidential candidate Wesley Clark, stated: "The travel, hotel, financial, immigration, health, or educational records of a person suspected by our government of planning terrorism may hold information that is vital."[1]

The website assures us that "MATRIX does not store dossiers on individuals"–as MATRIX technically doesn't really "store" anything, it simply searches and compiles from existing databases–"the MATRIX FACTS application does not track individuals," and "maintaining privacy is paramount to MATRIX." The security system, however, depends on the honor system. "User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of data."

Yes, law enforcement agencies must apply for licenses for access, and individual law enforcement personnel must submit to background checks and be "properly trained" prior to getting access to the data. But in the end, the proper use of the system is dependent entirely on the honor system, audits after the fact notwithstanding. "The MATRIX pilot project is guided by the premise that law enforcement agencies should not access, analyze or use personal information on U.S. citizens without a nexus to suspected terrorist or other illegal activity." "Should not," however, did not stop the Clinton administration from accessing the FBI files of political opponents.

MATRIX proponents, recognizing the sensitivity of the privacy issue, are quick to point out on their website that the "information available through MATRIX has been accessible to law enforcement for many years. Much of the information is available to the general public." It only contains "information already accessible to law enforcement from commercially available public records and state-owned data."

Besides, the question of the MATRIX-HIPAA connection notwithstanding, no one really expects his or her medical information to be private these days anyway. According to an official from the U.S. Department of Justice, which funds MATRIX, " 'There is no federal common law' protecting physician-patient privilege. In light of 'modern medical practice' and the growth of third-party insurers, it said, 'individuals no longer possess a reasonable expectation that their histories will remain completely confidential.' "[2]

The trend is clear and troubling. Government has coerced expansion of electronic medical records via Medicare and HIPAA. Through HIPAA, government has granted itself unprecedented increased access to information contained in electronic medical databases. And, through a public-private partnership, to avoid appearance of government ownership of the database information, government has now developed a way to search, compile, and analyze the data more quickly and thoroughly than ever before.

REFERENCES

[1] Behar R. Never heard of ACXIOM? Chances are it's heard of you. *Fortune*, Feb. 23, 2004, pp 140-148.

[2] Lichtblau E. Justice Dept. seeks hospital's records of some abortions, *New York Times*, Feb. 11, .Available at: www.nytimes.com/2004/02/12/politics/12ABOR.html?ex=1077593649&ei=1&en=c718d0b126e05dd0. Accessed Apr. 22, 2004.

Lawrence R. Huntoon, M.D., Ph.D., is a practicing neurologist and Editor-in-Chief of the *Journal of American Physicians and Surgeons*.