POLITICO

One of the main purposes of electronic health records is to encourage information sharing among doctors, so that patients can be looked after in a more holistic way. | Getty

Cyber ransom attacks panic hospitals, alarm Congress

By **ARTHUR ALLEN** | 05/25/16 05:00 AM EDT

When the Obama administration pushed out a $35 billion incentive program to pay doctors and hospitals to convert to electronic records, the idea was to modernize the health care industry, not serve it up on a platter to cyber criminals.

But now, American hospitals face weekly ransom threats. If they don't pay up, files get frozen, surgeries delayed and patients sent across town. One of these days, someone could die as a result. And no one in government has a clear plan to handle it.

Such are the unintended consequences of shovel-ready projects.

The incentive program, which started paying out cash in 2011, "thrust tens of

thousands of health care providers into the digital age before they were ready," says David Brailer, chief of health IT in the second Bush administration. "One area where they were woefully unprepared is security. It created thousands of vulnerabilities in hospitals and practices that lack the budget, staff or access to technical skills to deal with them."

Desperate hospitals have asked the feds for new financial incentives to boost their security. But Congress seems in no mood to cough up the necessary billions. It created a task force to come up with a report on how an alphabet soup of federal agencies can establish a chain of command for health care security.

Meanwhile, cybercrime attacks are mounting so rapidly that they challenge the financial stability of some health systems, according to experts in information security. The intrusions are interfering with efforts to improve data sharing in health care — and could even threaten patient safety.

Just this week, a Kansas hospital said it paid a large ransom to unblock frozen records — then was told it had to pay more in order to free all the files.

"It's only a matter of time before someone gets hurt," Sen. Sheldon Whitehouse (D-R.I.) said during a hearing this month after well-publicized ransomware attacks hit hospitals in Kentucky, California and the nation's capital.

Whitehouse and Sen. Lindsey Graham (R-S.C.) filed a bill this month to punish cyber criminals if their attacks result in health care system deaths or injuries. But first, they'd have to find perpetrators — in Russia, Eastern Europe or in hidden recesses of the Dark Web.

More rules won't help, Brailer says. Hospital licensing requirements and medical privacy laws already include extensive security requirements, but providers rarely follow best practices, he said.

The FDA and the Office for Civil Rights in the Health and Human Services department use penalties and guidance documents to push providers and device makers to use better "cyber hygiene."

Members of Congress also want hospitals to be more dutiful. "If you aren't following

good practices, the regulatory environment isn't going to save you," says Rep. Will Hurd (R-Texas), leader of the House Oversight cybersecurity subcommittee. While FBI and other agencies can do better at sharing threat intelligence, "health care has to help itself."

More federal inspections might increase readiness, but none of these measures attack the underlying problem — the massive gap between the industry's needs and its resources, Brailer said.

Meanwhile, hackers are launching billions of health care-focused attacks. One major health system was bombarded with a million emails in March alone seeking to implant ransomware in its computers. A small Kentucky hospital had 3,500 attacks on Mother's Day, according to Leslie Krigstein, vice president of the CHIME.

Last year there were 54 "zero-day," or brand new attacks; approximately once a week, in other words, hackers sent out an electronic bug so novel that no computer could recognize it.

Ransomware is of particular concern. In these attacks, hackers send out code that freeze computer files until the owner pays ransom in untraceable Bitcoins in exchange for a numeric decryption to unfreeze them. The attacks allow hackers to cash in quickly, whereas stolen medical records may be more difficult to monetize. (More than 100 million records were stolen in 2015 — some for sale on the black market or use in Medicare fraud, some by state actors, apparently for intelligence purposes).

Freakout in the C-Suite

For the first time, the threat of cyberattacks is grabbing the attention of senior health care executives, said Russell Branzell, CHIME's CEO, who says the executives are "freaking out" as we "enter into a security war for health care."

Cybersecurity legislation signed into law last year allows health care companies to share information about threats they've encountered without risk of being sued for any data breaches they reveal. Other privately run organizations also serve this purpose.

But complying with such recommendations can require major investments —

millions to hire new security teams and consultants and to buy new software. Added security spending might mean forgoing a new MRI system, or delaying the hiring of new nurses.

“Cyberthreats are knocking on your door every time you open your laptop or your phone,” said Ty Faulkner, a cyber consultant. “If you aren’t monitoring and checking your data, I question whether you are following good business processes.”

But "many of our members can’t afford the technology and tools they need at this point,” said Branzell. “It’s moving so fast that you could update everything, spend way more than you’re budgeting for, then the next wave of bad guy stuff comes up and you’re already behind again.”

"If you peer into the dark minds of a lot of hospital executives, they are rolling the dice as to where they allocate their budgets," said Clinton Mikel, an attorney with Health Law Partners.

Health care firms are spending vast sums to lure chief information security officers away from the financial and energy sector. The job description hardly existed in health care two years ago — now there are 500 just in Branzell’s organization.

Some companies are hiring security consultants on a semi-permanent basis, said Mac McMillan, co-founder and CEO of CynergisTek — one of those firms. If they don’t spend that big dough, many worry, a criminal breach of their information could result in bankruptcy levels of litigation.

Cyber insurance protects against some costs, but underwriters won’t write a policy unless the hospital system can demonstrate it is already spending plenty to defend itself.

Successful attacks are inevitable, security experts say. They talk of techniques such as compartmentalizing software, so hacks can be confined to a small area of the computer system, or programs that detect unusual computer activity within an organization, signs a bug has already penetrated the system.

“Most organizations can’t do that for themselves,” McMillan said. “More and more, people are saying to us, ‘I want a partner’ because cybercrime has become an industry.”

Medical devices: A ripe target?

The targets of attack within health care are practically limitless. “It’s hard to imagine a more complex and diverse environment than a hospital,” said Dave Palmer of Darktrace, a company whose technology searches for unusual behavior within networks.

“You have doctors and staff walking around with tablets, millions of dollars worth of scanners and sensitive machinery, all of it digitally integrated. You have visiting consultants there, maybe only a few days a week. Staff, porters, cleaning people.”

Users may not understand that bedside devices like monitors need to be secured, said Dennis Gallitano, a leading cyber attorney. Most cyber strategies are built around detecting and keeping out bugs, but “what about tunnels through the backdoor — a fax machine or pump?”

Device manufacturers are not required to meet the privacy and security standards of the Health Insurance Portability and Accountability Act (HIPAA); security experts say their protection is often lax, offering an attractive target for hackers looking for new ways into health systems. The FDA has begun working with manufacturers to improve device cybersecurity.

Security conflicts with transparency

One of the main purposes of electronic health records is to encourage information sharing among doctors, so that patients can be looked after in a more holistic way. Cyberthreats, some worry, could lead to a clampdown, because health care companies are leery of sharing data with institutions that might not be secure.

“There is very much a conflict in health care,” Branzell acknowledged. “The traditional model is, ‘Lock the world down.’ That doesn’t work in a world where we’re being asked to become more and more transparent and engage with our patients … With more patient engagement you’ve got people working from home on their Wi-Fi networks.”

Security should not be used as an excuse to block transparency, says Fred Trotter, a hacker and data journalist who serves on HHS’ Cybersecurity Task Force. In Trotter’s

view, the solution is to make a distinction between ordinary cybertheft and hacking that has patient safety implications.

Cyberattacks that might, say, cripple an MRI machine until a ransom is paid, he believes, should be classed with other health IT safety issues, such as poor usability or bad software design that could lead to medical errors.

An evil genius and a wayward duck (or chicken, or pig) are equally capable of starting a lethal viral epidemic. By the same token, it shouldn't matter whether a hacker or a stuck mouse button creates a clinical safety problem, he said.

HHS' Office of the National Coordinator for Health IT has tried for years to create a safety center where threats and problems with software can be shared, discussed and remedied.

Congress has refused to provide the budget.