Big cyber hack of health records is 'only a matter of time'

By DAVID PITTMAN | 7/1/14 2:17 PM EDT Updated: 7/1/14 3:44 PM EDT

The health world is flirting with disaster, say the experts who monitor crime in cyberspace. A hack that exposes the medical and financial records of tens of thousands of patients is coming, they say — it's only a matter of when.

As health data become increasingly digital and the use of electronic health records booms, thieves see patient records in a vulnerable health care system as attractive bait, according to experts interviewed by POLITICO. On the black market, a full identity profile contained in a single record can bring as much as $500.

The issue has yet to capture attention on Capitol Hill, which has been slow to act on cybersecurity legislation.

"What I think it's going to lead to, if it hasn't already, is an arms race between the criminal element and the people trying to protect health data," said Robert Wah, president of the American Medical Association and chief medical officer at the health technology firm CSC. "I think the health data stewards are probably a little behind in the race. The criminal elements are incredibly sophisticated."

The infamous Target breach occurred last year when hackers stole login information through the retailer's heating and air system. Although experts aren't sure what a major health care hack would look like, previous data breaches have resulted in identity and financial theft, and health care fraud.

While a stolen credit card or Social Security number fetches $1 or less on the black market, a person's medical information can yield hundreds of times more, according to the World Privacy Forum.

The Identify Theft Resource Center — which has identified 353 breaches in 2014 across industries it tracks, says almost half occurred in the health sector. Criminal attacks on health data have doubled since 2000, according to the Ponemon Institute, an industry leader in data security.

Health care is the industry least-prepared for a cyber attack, according to security ratings firm BitSight Technologies. The industry had the highest volume of threats and the slowest response time, leading the FBI in April to issue a warning to health care providers.

The industry "is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely," the FBI stated.

WHY HEALTH CARE AND WHY NOW?

The high value of health information makes it attractive to hackers.

A credit card can be cancelled within hours of its theft, but information in a patient's health record is impossible to undo. The record contains financial records, personal information, medical history, family contacts — enough iformation to build a full identity.

A patient's credit card information alone may be easier to hack from an unsuspecting hospital than from Target, Michael's or Neiman Marcus, experts say.

"Criminal elements will go where the money is," said Wah, who was the first deputy national coordinator in the Office of the National Coordinator for Health IT. "They're seeking health records not because they're curious about a celebrity's

blood type or medication lists or health problems. They're seeking health records because they can do huge financial, fraudulent damage, more so than they can with a credit card number or Social Security number."

Health care is the Johnny-come-lately to the digital world, trailing banks and retailers with decades of experience in cybersecurity. Most hospitals and doctors have gone from paper to electronic health records in the space of a few years while gobbling up $24 billion in federal incentive money paid out under the 2009 Health Information Technology for Economic and Clinical Health Act.

"Frankly, health care organizations are struggling to keep up with this," said information security expert Ernie Hood, of the The Advisory Board Company.

"It's not that they aren't trying," said Dennis Seymour, chief security architect at IT security consultant Ellumen. "It's just that they don't do the best job implementing it."