Weekly Checkup

Health Care and the Building Cyber-Security Crisis

CHRISTOPHER HOLT | MAY 28, 2021

Last week the Government Accountability Office published a report on cyber insurance, finding that demand for cyber insurance is growing in the health care industry. At the same time, however, "insurer appetite and capacity for underwriting cyber risk has contracted…especially in certain high-risk industry sectors such as health care." **Increasing cyberattacks on health care companies paired with growing demand for expanded telehealth services mean that health care policy conversations will increasingly need to focus on data security.**

In late April, cancer treatments for some U.S. cancer patients were disrupted when the Swedish-based Elekta—a company that provides precision cancer radiation treatment systems—had to take down its cloud system amid a data breach. While details on the type of breach have not been made public, at least 42 U.S. cancer centers had to delay scheduled treatments while the cyberattack was addressed. In early May, the San Diego-based Scripps Health hospital system experienced a cyberattack that is still impacting its operations. Details on the type of attack have again been withheld, but in the immediate aftermath, patient appointments were postponed and emergency patients were diverted. In another incident, last week the Alaska Department of Health and Social Services had to take down its website after a malware attack, disrupting access to a number of state services.

Cyberattacks have not been limited to the United States, either. Ireland's Department of Health has experienced two ransomware attacks in recent days, significantly disrupting the nation's government-run health care system. And in New Zealand this week, hackers stole patient records from the Waikato District Health Board—which serves 425,000 Kiwis—and released it to the media. All of these attacks have occurred in just the last month; looking back to last year, there are too many incidents to recount.

Overall, the threat seems to have increased during the COVID-19 pandemic. According to one report, there were 92 specific ransomware attacks impacting U.S. health companies and providers and impacting more than 18 million patient records in 2020 alone. **All told these attacks are estimated to have cost the health care industry $20.8 billion in 2020. Another recent report found that ransomware attacks targeting the U.S. health industry increase 123 percent from 2019 to 2020.**

There are a lot of reasons why health care companies and providers face a unique threat from cyber-attackers. For one, the data these companies hold are worth a fortune. Patient records provide a treasure trove for identity thieves, and that's not considering the potential for blackmail and ransom demands related to personal health information. But health care providers are also uniquely at risk. Medical devices are increasingly connected and do not have the same levels of security that devices such as computers and even smartphones have. Further, health care workers are simply not well trained to be aware of cyber threats. And health systems often have outdated networks, making them even more vulnerable to attack. **In short, health systems provide a unique combination of a wealth of data and insufficient security frameworks.**

One positive of the COVID-19 pandemic has been the rise of telemedicine with its opportunities for both savings and patient convenience. But **if policymakers want to build on the opportunities for expanded telemedicine post-pandemic, they're also going to have to make serious efforts at addressing cyber-security in health care.**

VIDEO: THE EFFECT OF H.R. 3 ON DRUG PRICES AND INNOVATION

AAF's Director of Health Care Policy Christopher Holt explains why Democrats' proposed drug-pricing legislation, H.R. 3, will restrict drug availability and innovation.

??

FROM TEAM HEALTH

Video: The Current State of Public Health Relations
Christopher Holt discusses the recent fall in confidence in public health officials amid the COVID-19 pandemic.

TRACKING COVID-19 CASES AND VACCINATIONS

Jackson Hammond, Health Care Policy Analyst

To track the progress in vaccinations, the Weekly Checkup will compile the most relevant statistics for the week, with the seven-day period ending on the Wednesday of each week.

Week Ending:	New COVID-19 Cases: 7-day average	Newly Fully Vaccinated: 7-Day Average	Daily Deaths: 7-Day Average
May 26, 2021	21,627	565,410	437
May 19, 2021	27,818	975,023	504
May 12, 2021	34,468	1,179,683	569
May 5, 2021	45,657	1,380,349	611

April 28, 2021	51,847	1,417,848	634
April 21, 2021	60,849	1,463,671	664
April 14, 2021	67,772	1,712,577	665
April 7, 2021	63,772	1,550,441	586
March 31, 2021	63,657	1,353,953	725
March 24, 2021	57,355	953,497	734
March 17, 2021	52,708	1,014,026	890
March 10, 2021	54,107	945,467	1,166
March 3, 2021	61,147	902,095	1,439
February 24, 2021	64,630	835,637	1,802
February 17, 2021	74,218	736,664	1,941
February 10, 2021	99,151	692,608	2,417
February 3, 2021	129,840	477,719	2,703
January 27, 2021	156,744	332,246	3,137

Sources: Centers for Disease Control and Prevention Trends in COVID-19 Cases and Deaths in the US, and Trends in COVID-19 Vaccinations in the US

Note: The U.S. population is 332,364,254.

WORTH A LOOK

The Hill: Google, hospital chain partner in push to boost efficiency

Axios: A faster way to track COVID variants