FAST COMPANY

February 6, 2015

Why The Anthem Security Breach Was Such A Wake-Up Call For The Health Industry

By: Luke Dormehl

Anthem, the second largest health insurance provider in the United States, revealed on Thursday that its records have been compromised by hackers—resulting in the possible leaking of names, birthdays, addresses, Social Security numbers, and employment data for up to 80 million present and former customers.

Although no medical information appears have been stolen, with the exception of customers' medical identification numbers, the attack is being viewed as a much-needed wake-up call for the heath industry.

"Cybercriminals do view health care organizations as a soft target," says Lynne Dunbrack, research VP for IDC Health Insights. "They classically have not invested too heavily in information-technology in general, and specifically in security. Going hand in hand with that is the value of medical information on the black market, which has long since exceeded the value of personal identifiers for financial data. To give you an idea, financial records may fetch just a couple of dollars, whereas medical information routinely sells for $200. That's a real incentive for cybercriminals."

Worries about the security of health care data is a growing issue—accompanying the increasing digitization of medical records, combined with the still more recent shift toward cloud-based record holding. Anthem's mess is far from the only recent example of troubling privacy concerns regarding health data. In 2010, the C**oalition Against Insurance Fraud** reported that 1.4 million Americans were victims of medical identify theft, representing a significant increase from the 500,000 one year earlier.

Stolen medical data can be particularly problematic for consumers. Whereas credit-card fraud may be corrected in a relatively straightforward manner, it can be tougher to identify that medical data has been breached. Maximum insurance payout limits may be reached as a result of fraudulent claims, and this might only be discovered when a consumer's claims for legitimate services are denied.

Worse, consumers' medical records could become compromised with falsified diagnoses or procedure codes following data-theft incidents. In a worst-case scenario, vital information related to allergies or blood type could be compromised, with the wrong drugs or blood products administered to a patient as a result.

Others have expressed concern about what appears to be the misuse of private medical data. Last month, Ricardo Alonso-Zaldivar and Jack Gillum of the Associated Press reported that Healthcare.gov has shared user data—possibly including information about age, income, and whether or not a person is pregnant—with tech companies such as Google, Twitter, and Facebook. Although there is no evidence that this data has been misused, it is still likely that this will irk some individuals.

TROUBLE TO COME

Hacking remains the number-one concern for medical data misuse, but the growing role of tech companies in health care underlines just how much today's medical system relies on technology. IDC Health Insights claims 70% of health care organizations worldwide will invest in mobile health tech such as apps, wearables, remote monitoring, and virtual care by 2018. Apple, Microsoft, Samsung, and Google all have high-profile health initiatives that will only expand as health-tracking technologies in Apple Watch and other wearables gain momentum.

"I think it's safe to say that all of the major players, including Amazon, Microsoft, Google