Prescription for the ailing healthcare industry

It's not: "take two aspirin and call me in the morning"
It is: STOP being a prime target for data breaches

Are you aware of these alarming statistics?

- Over 100 million healthcare records from more than 8,000 devices in more than 100 countries were compromised in 2015.[1]
- Data breaches cost the healthcare sector $6.2 billion—with nearly 8 out of 10 healthcare institutions hit by 2 or more data breaches in the last 2 years and 45% affected with more than 5 breaches.[2]
- Nearly 1.6 million people had their medical information stolen from healthcare providers in 2014.[3]
- Four out of five U.S. healthcare executives admitted their IT has been compromised by hackers and 53% of providers admitted to not being prepared against attacks.[4]
- The percentage of healthcare organizations attacked by cyber criminals rose to 40% in 2013— from 20% in 2009.[5]
- In 2016 there were 450 breaches affecting 27 million patient records—with 120 outside hacking incidents versus 200—over 65% more—inside threats.[6]
- 47% of healthcare providers and plans said they had instances of security-related HIPAA violations or cyberattacks that compromised data—compared with 37% in the prior year.[7]

- Data breaches could cost the healthcare industry more than $300 billion of cumulative lifetime patient revenue over the next five years.[8]

Healthcare CIOs and CISOs are under cyberattack daily, including spoofing and spear phishing. Recent WannaCry, Petya and NotPetya attacks are significantly impacting the industry.

5 reasons why the healthcare industry has a bull's eye on its back

1. Underspending on cybersecurity **programs**[9]**—**investments against cyberattacks will reach $10 billion worldwide by 2020—10% under the total spend on critical infrastructure security.[10]

2.High demand for black market medical records—an electronic health record (EHR) is worth more on the black market than financial data—EHRs sell for hundreds or thousands of dollars, compared to 10 cents for a stolen Social Security number or 25 cents for a credit card number.[11]

What makes an EHR so valuable? It includes all personal demographic information, work history, names and ages of relatives, financial data and past medical history—information that could be exploited by hackers.

3.Ransomware Threats—infects a healthcare organization's IT system, preventing file access—unplanned downtime may cost nearly $8,000 per minute per incident and explains why most hospitals would rather pay than deal with major operational losses.[12]

4.Bring Your Own Device (BYOD) Policy—81% of healthcare providers allow doctors and staff to use their own iPads and other mobile devices at work—but 46% indicate they're not doing anything to secure these mobile devices and 54% say they have no confidence that the employee-owned mobile devices used at work are secure.[13] Plus, 66% of health apps that send identifying information over the Internet don't use encryption and 20% don't have a privacy policy.[14]

5.**Employee Negligence—**the majority of unauthorized access to EHRs comes from insider attacks. They involve nurses or doctors, billing specialists, or administrators who abuse their access for revenge, financial gain or curiosity.[15] Employee cybersecurity training can reduce the risk of a cyberattack from 70 to 45%.[16]

What are they after?

PII and PHI. That's Personally Identifiable Information and Protected Health Information. All the stuff that's in an EHR. A patient's history and personal data go back decades—and patients rely on their healthcare providers to protect their information. If there is a breach, hackers can potentially blackmail a patient for a lifetime, threatening to reveal PHI.

Where is it happening?

Hospitals, clinics and healthcare providers across the country, like Anthem BlueCross BlueShield, and others listed in the report the biggest healthcare breaches of 2017 (so far).

How does HIPAA fit in?

Health Insurance Portability and Accountability Act (HIPAA) compliance on its own does not ensure PHI security. And HIPAA does not cover patient data once it is downloaded from a patient portal—the FTC is responsible for protecting privacy and data security.

HIPAA requires healthcare organizations to report security breaches that result in the exposure of patient data. The maximum penalty for a HIPAA violation is set at $1.5 million by the HITECH Act. Violations can also result in criminal charges, state penalties, and patients may choose to pursue litigation.

The medicine for the cure

Breaches like Anthem's—where an employee sent himself a file of over 18,000 member PHIs, including Medicare ID and contract numbers, health plan IDs and enrollment dates—could have been prevented with the right solution in place. When it comes to something as personal as medical records, the focus should be on the mission-critical task to implement a solution to protect content at rest, in use and in transit to prevent a data breach in the first place—that's the cure to stop being a prime target for data breaches—the aspirin is for your headache, if you don't follow the prescription.

The GigaTrust™ flagship service, GigaCloud™, delivers persistently protected emails and documents for collaboration anytime, anywhere, on virtually any device for the healthcare industry. GigaCloud is the first and only secure email and document protection, consumption, and collaboration service that is an easy-to-use, easy-to-deploy private or multi-tenant cloud service powered by the Microsoft – Active Directory Rights Management Services (AD RMS) security ecosystem.