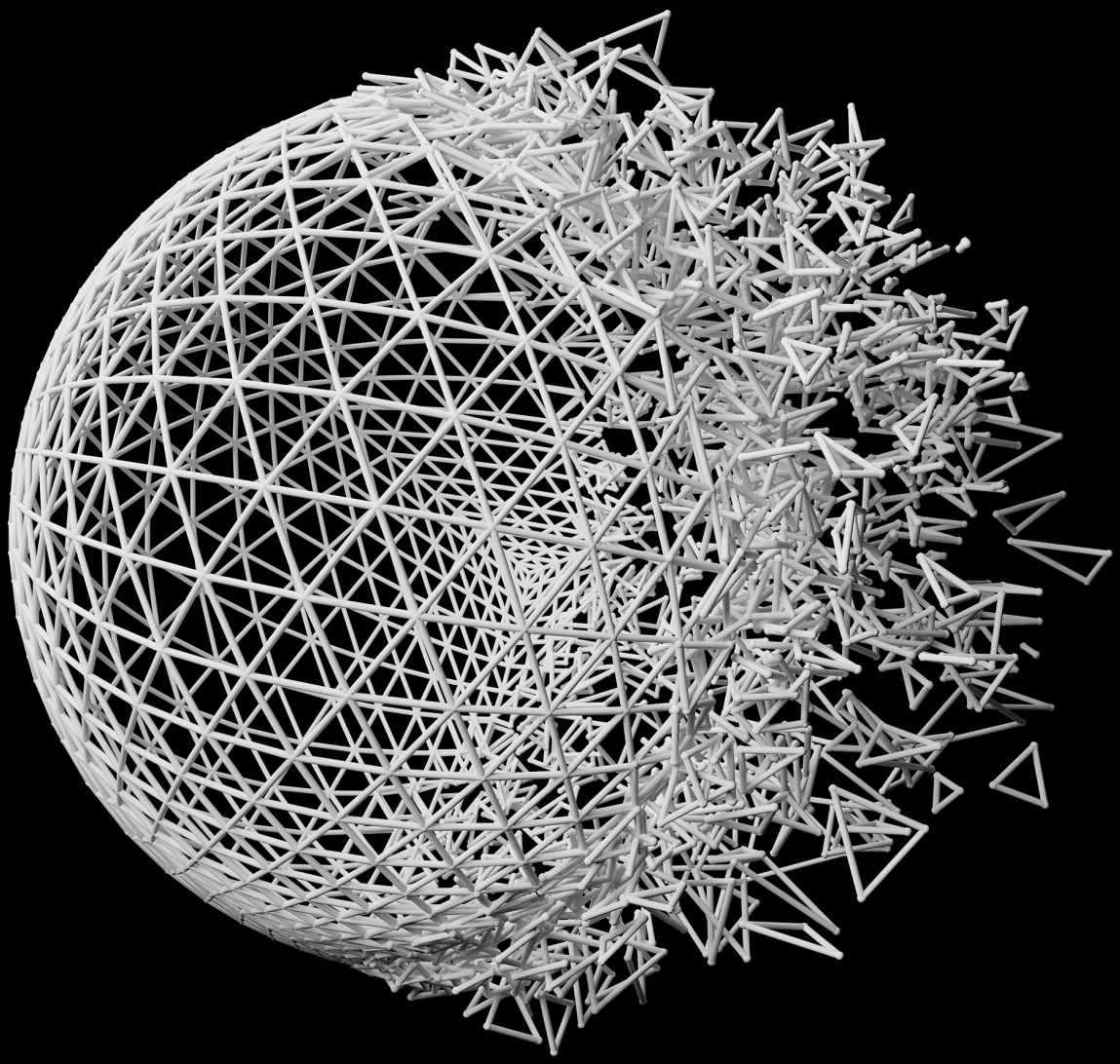
Deloitte.

Deloitte Center *for*
Government Insights



The Looming Wave of Cyber Fraud in Health Care

By: Brien Lorenze; Dan Olson, CFE; and Eric Dull, MS


ID:
Date: May 31 2005
Study: 50413
Series: 603
Image: 167
TR: 0.00
TE: 0.00

Health-care fraud exists when unscrupulous individuals or entities seek to exploit vulnerabilities and loop-holes in payment systems through deception for their unlawful financial gain. The unsettling news is that with cyber crime, the problem of health-care fraud is more complex and difficult to detect. The cyber world allows perpetrators to be anonymous, and employ nuanced, sophisticated and nefarious methods to exploit individuals and entities very quickly. By operating in a non-physical environment and from disparate locations around the world, perpetrators are nearly invisible to their victims while committing crime and for practical purposes untouchable to law enforcement after the fact.

Cyber Fraud Is Evolving

Cyber fraud is often used synonymously with data breaches, but it is only one step in an increasingly complicated dance to use the Internet to steal from government, insurance plans, doctors and hospitals. The traditional physical and automated nature of financial crime is fading into cyber. Identity theft and health-care fraud are not new; however, the methods used to enable the theft of information and money are becoming more difficult to detect. Because costs to attempt cyber fraud are low, the velocity at which fraud schemes are tried and refined is accelerating. Cyber enables fraud to be perpetrated outside the legal jurisdiction in which it takes place—out of a foreign country without extradition, or spread throughout the country by a network of individuals who never meet. And, with the advent and expanded use of virtual currency (e.g., Bitcoin), "following the money" becomes even more challenging.

A Compelling Reason to Take Action

The United States currently spends $3 trillion per year on health care—$9,024 per capita—while other advanced economies rarely spend above $5,000.[2] The Institute for Medicine estimates 30 percent of our health-care spend is lost to fraud, waste and abuse.[3] The inevitable conclusion: there is nearly one-trillion dollars in savings to realize across the system.

With health-care fraud increasingly in the cyber realm, and outpacing government and industry attempts to mount defenses, matters may well get worse before they get better. The evolution of systems to administer health care is advancing faster than our security solutions; and we must adapt to protect against technology after it is already part of our environment.

Why is health care a target?

1. It amounts to $3.2 trillion or 17.8 percent of U.S. GDP. [1]
2. It is inherently vulnerable to collusion and misrepresentation, i.e. the "payer" is not the one receiving the service.
3. Payments are mandated to be paid electronically and, thus, subject to cyberattack.

Although the world is increasingly interconnected, hackers are mobile and difficult to detect. They could be sitting next to you at the park or even be a malicious insider working within your organization. James Socas reports in Healthcare IT News, "personal information of nearly half of the U.S. adult population has been compromised in some manner by a data breach of their healthcare insurance provider."[5] While there have been high-profile successes, we only know what we know. It is highly likely schemes are being committed that have not yet been identified.

Government and industry efforts to address the challenge are mixed. Many organizations lag, not yet sufficiently protecting against hacks, and still using rudimentary rules-based monitoring, tip lines and audit as their lines of defense. Others are innovating, introducing sophisticated walls of defense, and using predictive modeling and data analytics to identify likely fraud. But, nobody is ahead of the impending cyber fraud wave.

Eighty percent of providers admit they recently experienced a significant security incident.[4]

Scenarios presented (the names and circumstances are illustrative) demonstrate how cyber fraud is evolving and leveraging new methods for enabling traditional schemes. The progression shows how fraud conducted via the Internet by one person new to criminal activity grows into a sophisticated fraud scheme lurking in the shadows of the dark web.

SCENARIO 1—Single perpetrator: legitimate pharmacy electronically submits false claims.
Ryan is the pharmacy manager and part owner of Hometown Pharmacy. His personal debt is mounting and college tuition payments for his three children loom. Ryan notices an increase in the number of benzodiazepine and opioid prescriptions processed and dispensed. Due to the volume of these prescriptions, he is not always able to fill the quantity prescribed and asks his customers to return to pick up the balance of their prescription. He bills the insurance carrier for the full amount, rather than prorating the prescription for the partial fill. He notices that customers rarely return to pick up their remaining prescription, so Ryan restocks the drugs in his inventory without crediting the insurance carrier for the difference. Over time, he systematically fills partial prescriptions, bills for full prescriptions and sells the "restocked" drugs for cash without a prescription, keeping the cash for himself.

SCENARIO 2—Identity theft and the dark web enable and accelerate misrepresentation.
Sue is a physician who recently started her own practice. While in medical school, she became hooked on benzodiazepines and opioids to help her get through the stress and long hours of her residency. Sue purchased the drugs she needed from Ryan, whom she met through a mutual friend. With a clear understanding of the billing process for health-care services and a proficiency with computers, Sue sees an opportunity to support her habit and make additional money to supplement her new practice.

Sue and Ryan collude to expand the scheme. Sue purchases a patient list through the dark web (the modern black market) with virtual currency. The information includes patient name, Social Security number, date of birth and insurance carrier, as this list resulted from a hack of the carrier's eligibility system. She submits an office-visit claim for each patient on the list to see whether the claim will be paid. The insurance carrier's claim system assists Sue in "cleansing" the list by notifying Sue when a claim is rejected, including providing the reason for the rejection, such as deceased or ineligible. Now that Sue has a clean list, Ryan and Sue have the green light to bill through a "bust-out" scheme to prescribe and bill for unnecessary benzodiazepines and opioids.

Sue submits electronic prescriptions to the Hometown Pharmacy; and Ryan submits the pharmacy claim to the insurance carrier. The drugs are diverted to Sue directly or sold for cash. Sue encourages several of her real patients to feign symptoms to obtain the illicit drugs. Sue becomes known to her patients as someone willing to prescribe benzodiazepines and opiates unnecessarily; and, as a result, she sees a rapid increase in her patient load requesting these prescriptions. Sue directs these patients to fill their prescriptions at Hometown Pharmacy.

SCENARIO 3—Next generation: sophisticated criminal enterprise hidden in the shadows of the dark web and virtual currency transactions—the saga expands.
Harry is a seasoned hacker who spends time on the dark web—monitoring forums, analyzing credential dumps, running small-time schemes and generally getting into mischief on the Internet. Harry sees a posting from Sue asking how to use a virtual currency client that wasn't working on her mobile device. This technological failure was preventing Sue from accepting virtual currency payments from "patients" purchasing prescription drugs from Ryan's extra inventory. Harry helped Sue solve her technical problem; Sue offers Harry a virtual currency payment in exchange for his services. During the technical assistance, Harry installs a Remote Access Tool (RAT) on Sue's mobile device.

While examining Sue's email using the RAT, Harry realizes Sue is a doctor and he steals Sue's credentials. Harry creates a new office location on Sue's provider profile with a separate bank routing number for carrier payments. Harry uses the available data breaches to commit identity theft on a large scale and repeats Sue's process of cleansing a candidate patient list. Harry then submits medical claims with Sue's stolen credentials. Sue's credentials are only one of the many physician credentials in Harry's pocket. Harry is able to perpetrate a larger-scale fraud than Sue because he is more technically savvy, has access to more data dumps, and is much harder to catch and prosecute than Ryan and Sue, who know each other and are geographically close to each other.

Harry now sets about recruiting accomplices through postings on dark web forums. These accomplices are located across the United States, eliminating hotspots of fraud that are more easily detected. Harry then purchases fake identification documents from vendors on the dark web for the patient information he is using to bill the

insurance carrier. Harry submits e-prescriptions to high-traffic pharmacies in locations near the accomplices; the accomplices use their high-quality false identifications to pass pharmacy staff scrutiny and collect the prescription drugs. The accomplices pick up the prescriptions and mail the pills to a number of post office boxes that Harry maintains. Harry then sells the pills to a worldwide customer base via the dark web. Harry collects payment using virtual currency and pays his accomplices via virtual currency.

Harry is a ghost with a criminal network virtually untraceable in the dark web.

No Simple Solution

There is not a simple solution to the challenge of program integrity in health care, and keeping up with ever-emerging schemes of increasing complexity requires extraordinary vigilance and enhanced capabilities. Still, there are prevention and detection "counters" that should be part of a comprehensive solution. Basic recommendations include:

- continue to enforce strong IT security practices, including network access controls, firewalls, and anti-virus software;
- strengthen collaboration among industry groups, commercial entities, government regulators and law enforcement to address vulnerabilities; establish counter-intelligence programs to monitor for insider threat;
- utilize predictive modeling and data analytics to detect anomalies and guide the use of forensic and investigative resources;
- build stronger pre-payment monitoring systems, integrating claims, third-party data sets and identity theft patterns to strengthen decision support; and
- establish models for outbound monitoring.

For example, agencies can counter the scheme depicted in scenario 1 by instituting both pre- and post-payment analytics. One tactic of a post-payment analytic is identifying prescriber outliers who fill a significant number of partial fill medications. A second, would be to further evaluate that same set of providers to determine if a corresponding credit was made for the partial fill prescription. A pre-payment methodology would monitor existing prescription inventory levels and disallow new inventory shipments when an adequate supply of medication is stocked at the pharmacy. From a financial management perspective, these methods would provide cost savings and cost avoidance to strengthen internal controls to thwart the fraud perpetrator.

Instituting pre- and post-payment rules and models that evaluate paid and rejected claims would help in scenario 2. In this case, a rejected claims analysis is a key determinate of someone exploring the payors system to learn where they can exploit it. Sue gains priceless information from the insurance carrier when they educate her as to why the claim was rejected. Conversely, through continuous monitoring and machine learning, the fraud analyst can identify emerging schemes and characteristics of bust-out schemes before they occur. Armed with this information, the financial management perspective provides both cost savings and cost avoidance to strengthen internal controls and fraud controls to thwart the fraud perpetrator.

Government agencies can counter the criminal network depicted in scenario 3, through behavioral analytics on prescription databases to reveal indicators that suggest criminal activity. Through the behavioral sciences we seek inconsistencies in established patterns of behavior and activities (e.g., drugs not usually prescribed by a particular doctor, or time of prescription occurring while office is closed). We might also look for examples where Sue violates a doctor's "homerange" features, and this extends to indicators that would show that she has no reason to interact with Harry if not for illicit activities.

The risk management community must anticipate new fraud schemes before they are unleashed. The recommended measures will not eliminate the threat, but they can make it more difficult for the attacker and move cyber fraud risk management to a more preemptive and proactive posture.

Brien Lorenze is a principal in the Regulatory, Forensics & Compliance practice of Deloitte Transactions and Business Analytics LLP, and the global public-sector leader. He specializes in monitoring and detection of financial crime, including improper payments, money laundering, fraud, sanctions evasion, and the financing of terrorism.

Dan Olson, CFE is a senior manager in Deloitte's Risk and Financial Advisory practice. He has worked for more than 25 years in health care fraud examination, developing and implementing predictive analytics for Medicaid, Medicare and commercial payer plans.

Eric Dull, MS, is a specialist leader at Deloitte & Touche LLP. As a data scientist, he leads teams developing cyber solutions that utilize high-performance and cloud computing architectures.

Endnotes

1. Centers for Medicare & Medicaid Services National Health Expenditure Data: www.cms.gov/research-statistics-data-and-systems/statistics-trends-and-reports/nationalhealthexpenddata/ nationalhealthaccountshistorical.html; accessed Aug. 10, 2017.
2. www.pgpf.org/chart-archive/0006_ health-care-oecd
3. "IOM Report: Estimated $750B Wasted Annually In Health Care System," Kaiser Health News, Sept. 7, 2012.
4. Health Information and Management Systems Society 2016 HIMSS Cybersecurity Survey.
5. "Growing pains: Cybercrime plagues the healthcare industry" by James Socas, Healthcare IT News, Dec. 21, 2015.

Deloitte.