How COVID-19 has opened the door to an increase in remote scams

The state of telemedicine fraud

INSURANCE INSIGHTS

BAE SYSTEMS

Introduction

Medical fraud has a long and not-so-illustrious history dating back to the "snake oil" salesman of the 18th century. Today, the modern fraudster has a huge repertoire to draw on, ranging from paper or staged accidents to fake injuries at work and fictitious claims related to defective or harmful products. The proliferation of medical identity data on the cybercrime underground and the coming together of medical and legal entities to conduct scams makes schemes more organised and harder to detect.

COVID-19 has kicked the door wide open, providing new opportunities for organised crime groups to commit widespread medical insurance fraud and creating the perilous economic conditions which could persuade many legitimate businesses and individuals to act dishonestly themselves. Perhaps one of the biggest trends we're seeing at the moment, especially in the US, is that of telemedicine fraud. COVID-19 restrictions and patient preferences have led to surging numbers of remote medical appointments, and with them, increased attempts of various types of medical fraud.

At BAE Systems' 2020 Global Insurance Fraud Summit in November, we heard from several experts about the scale of the challenge facing insurers in this space, and what the industry can do to fight back.

The scale of telemedicine

Telemedicine has been around for years. In its purest form, it means any healthcare services that are conducted remotely, usually via video conferencing or similar technologies. However, like many digital trends, the pandemic has spurred take-up on an almost unprecedented scale. Figures cited by McKinsey claim that[1]:

- Telehealth visits have soared by 50-175 times versus pre-COVID
- Nearly two thirds (64%) of providers are now comfortable using the technology
- Just 11% of consumers used telehealth in 2019, but now 76% are interested in using it going forward

It's perhaps not surprising that Forrester predicts: "virtual care visits will soar to more than one billion this year, including 900 million visits related to COVID-19."[2]

However, with large numbers of users, and money to be made, inevitably there will also be fraud.

> It’s perhaps not surprising that Forrester predicts: “virtual care visits will soar to more than one billion this year, including 900 million visits related to COVID-19.”

What types of telemedicine fraud are there?

According to Fred Burkhardt, Supervisory Special Agent at the National Insurance Crime Bureau (NICB), medical fraud accounts for around $60 billion of the $80 billion in insurance fraud committed in the US every year. Telemedicine-related scams are just one of over 13 categories of medical insurance fraud.

The fact that the patient is not in the same room as the physician opens the door to two main types of fraud: fictitious billing, and unnecessary referrals, prescriptions and other services. Burkhardt lists the main types of telemedicine fraud as follows:

Phantom billing – if there’s no patient to sign in and create a record of their appointment, clinicians feel it’s easier to bill for appointments that never happened. Some of these may be for real patients, but they could also be for patients whose identity data was obtained illegally. Healthcare is a highly targeted sector. According to the Identity Theft Resource Center’s (ITRC) 2019 Data Breach Report, there were 525 medical and healthcare data breaches in 2019, exposing over 39 million sensitive records.[3]

Upcoding – this is similar to the above, where a doctor inflates the time and complexity of a consultation in order to fraudulently bill more from the insurer.

Unnecessary prescriptions – these are deliberately written out by a doctor so they can charge the insurer more. Or, in the case of opioid abuse or similar, a physician may continue to write prescriptions out to retain a patient, even if their health may suffer as a result.

Unnecessary Durable Medical Equipment (DME) – doctors may bill for DME that the patient doesn't need, under the pretext that it's difficult to tell for sure without an in-person physical exam.

Unnecessary diagnostic referrals – similar to the above scenarios, the clinician sends the patient for MRIs, X-rays, and possible referrals to dieticians, physiotherapists and others because it "seems like the patient needs them." In reality, they are inflating their own takings and those of their "buddies" in adjacent practices with referrals back and forth, says Burkhardt.

Pain management – these programs will combine extra prescriptions for painkillers with referrals for physiotherapy and other appointments as per the above examples. Doing so will also help to inflate a claim for an injury settlement, which may be useful if a medical practice is working alongside a chosen attorney to commit organised fraud. It's a win-win for both parties: more billing for the doctor and a higher pay-out for the attorney.

In many cases, the remote, digital nature of the crime makes it easier for clinicians to justify. "No harm no foul, it's just done through the computer," says Burkhardt.

Increasingly, telemedicine is not an opportunistic type of fraud, but one that is highly organised and involves multiple parties including attorneys, clinicians and telemedicine providers. One case revealed by the US Department of Justice in April 2020 involves a $60 million scheme in which over 20 individuals were charged. In it, a telemedicine company allegedly provided kickbacks to physicians and nurses in return for fake orders of DME, which could then be sold to equipment providers and billed to Medicare.[4]

Time to take action

COVID-19 has not only opened the door to a surge in telemedicine use and fraud. It has also ossified the criminal justice system, making it harder for insurers and industry groups to pursue cases and get new legislation on the books, according to Matthew Smith, Executive Director of the Coalition Against Insurance Fraud.

"At least in the US, most insurers thought they had a decade to prepare for telemedicine," he says. "That evaporated immediately in March 2020 and insurers had to immediately determine how to handle telemedicine issues and identify and investigate insurance fraud that may be related."

Their efforts may be complicated by the lack of recording and reporting capabilities on some of the messaging platforms that are allowed for telemedicine appointments, he adds.

However, there are things that insurers can do today, even as this type of fraud rapidly evolves. According to BAE Systems' Dennis Toomey, they include:

- **Vigilance** in looking at claims and billing codes: check whether injuries match the treatment and vice versa, whether the injuries themselves make sense, and if the provider has a history of fraud or suspicious claims. Insurers should also be on the lookout for template billing, where almost identical claims are filed en masse, and physician licenses that may have expired.
- **Enterprise-grade solutions** can help to bust traditional insurance siloes which separate internal auditing, underwriting, sales groups and other functions. By bringing them together and applying advanced analytics to underlying data, insurers can spot the patterns that indicate organised fraud.
- **Patient action** is the best first line-of-defence. By questioning their treatment and ensuring insurers are billed correctly, they can make a big difference. After all, this is not a victimless crime: fraud makes everyone's premiums potentially hundreds of pounds higher.

> "In 2021, there'll be significant demand for people wanting to take part in these scams and a tenacious, professional and willing supply chain that is still there to try and exploit it."
>
> Ben Fletcher, MD, IFB.

Telemedicine is here to stay. It will long outlast the pandemic, and so will associated fraud, unless insurers adapt their detection strategies. New regulations and standards may be on the way in the US, and a major effort has already begun to understand the impact of COVID-19. Going forward, closer ties between all stakeholders—insurance fraud teams, cybersecurity and threat intelligence practitioners and law enforcers—will be necessary to improve our collective response.

[1] Telehealth: A quarter-trillion-dollar post-COVID-19 reality?, Oleg Bestsennyy, Greg Gilbert, Alex Harris, and Jennifer Rost, McKinsey (29 May 2020)

[2] US Virtual Care Visits To Soar To More Than 1 Billion, Forrester (10 April 2020)

[3] Data breaches in the healthcare industry continue due to availability of valuable information, ITRC (11 August 2020)

[4] Telemedicine company owner charged in $60 million fraud scheme, DoJ (23 April 2020)

We are

BAE SYSTEMS

At BAE Systems, we provide some of the world's most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.

Global Headquarters
BAE Systems
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

BAE Systems
19, Boulevard Malesherbes
75008 Paris
France
T: +33 (0) 1 55 27 37 37

BAE Systems
Mainzer Landstrasse 50
60325 Frankfurt am Main
Germany
T: +49 (0) 69 244 330 040

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com | W: baesystems.com/5G

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai