IN RUDE HEALTH

Philipp Pointner *gives his prognosis on how the healthcare industry is having to adapt against fraud in the post-COVID-19 landscape*

COVID-19 has led to significant shifts in the way individuals conduct daily activities, with the health space being one of the most prominent areas experiencing radical changes. Take for example GP appointments: prior to the Coronavirus outbreak, video appointments made up only 1 percent of the 340-million or so annual visits to the GP at the NHS. However, as the virus continues to spread, companies like Push Doctor and Docly have seen a surge in demand of their online services with an increase of up to 100 percent week on week.

Many of us are taking to telemedicine like ducks to water, and we're likely to see this trend continue into the post-lockdown era. Prior to COVID-19, the global market for telehealth was expected to grow by $95.72-billion between 2020 and 2024 at a CAGR of more than 25 percent. Despite the Government stating that the NHS is "open for business as usual," there are still millions of people across the UK socially distancing themselves in some form. Many are turning to online medical advice and services instead of visiting a local clinic or hospital. As a result, it's safe to assume that the global telehealth figures will see a rapid spike in initial estimates as the public adapts to new ways of interacting with healthcare providers, thus turning telehealth into the modus operandi even when the pandemic subsides.

IT IS CRUCIAL THAT ALL HEALTHCARE INSTITUTIONS ESTABLISH SECURE KNOW YOUR PATIENT PROCESSES

However, this transition into a more online world means that we need to become more cautious of the associated risks, including how we're potentially opening the door to fraudsters who are looking to exploit this new virtual process. The healthcare space is particularly vulnerable to impersonation fraud. Over 1-billion patient health records can be obtained on the Dark Web and more records are being added daily. Due to the personal and sensitive information embedded within a medical record, compared with other electronic databases, they are an especially lucrative target for cybercriminals, and as a result, cost up to $1,000/record on the Dark Web. That's 10 times more expensive than the average credit card record.

Data breaches are becoming more and more common in today's modern world. For example, over 800-million records were breached in the UK in March 2020 alone. Fuelling the vulnerability of the healthcare space is a deluge of breaches. The average cost of a data breach in the healthcare industry is £5.2-million globally, compared with £3.2-million across all verticals. What's more, 67 percent of UK healthcare organisations experienced a cybersecurity incident during 2019, and over the last decade, there have been over 2,550 healthcare breaches, which have impacted more than 175 million medical records.

This demonstrates the dangers of operating a business that deals with personal identifiable information (PII), which not only includes the patient's age and address but also far more sensitive information like medical histories and prescription details. It is this level of detail that leaves individuals and healthcare providers vulnerable to identity, insurance and prescription fraud. It comes as no surprise then that the healthcare industry is the most breached industry.

The first six months of 2019 saw the number of records exposed by data breaches rise 52 percent compared with the same period in 2018. Paired with this, the Dark Web is also growing, said to now be several orders of magnitude larger than the surface web because criminals are finding more advanced ways to easily obtain PII through unscrupulous means. And these numbers are likely to increase in the wake of COVID-19. In fact, the percent of suspected fraudulent digital transactions rose 5 percent from 11 March to 28 April when compared with 1 January to 10 March, 2020 according to a recent TransUnion study. More than 100-million risky transactions from 11 March to 28 April have been identified.

Now that many transactions have shifted online, fraudsters are taking advantage and healthcare organisations must adapt. The organisations that will weather this storm will be those leveraging fraud prevention and digital authentication tools that provide better fraud detection and reduce the perceived friction of patients.

However, while the breached organisation has an obligation to protect patients in an online world, individuals have a critical role to play in protecting their own digital identities too. Re-using the same password for multiple accounts is the main problem here, whether that is to login to your GP's portal or your Facebook account, it is this practice that leads to the success of credential stuffing attacks. This is where fraudsters buy email addresses and their corresponding passwords en masse on the Dark Web, then employ bots to try and access thousands of websites with those same login details in the hope of striking gold. Given the success rates of credential stuffing, patients need to think about password hygiene and recycling when it comes to setting up an account with a telemedicine provider. But to truly reduce this risk, and protect patients' valuable data, it is crucial that all healthcare institutions establish reliable, secure and accurate Know Your Patient (KYP) processes.

The average cost of a data breach in the healthcare industry is £5.2-million globally

A KYP strategy is a much more sophisticated way of protecting patient data, and here's why. Usually, if we were to visit a physical GP, we'd be expected to bring some form of proof of address, such as a utility bill, and Government-issued identification (eg a passport or driver's license). Often, we also need to physically come into the doctor's surgery to give our blood pressure, weight, *etc.* so that they have a record on file. However, with telemedicine, this type of identity proofing to ensure that the patient is who they say they are can be done in a virtual setting, and is arguably now more important and safer for medical professionals.

For example, a fraudster could have bought stolen credentials on the Dark Web to then impersonate a patient to access a medical service. If this did happen, which is a very real possibility, the fraudster that stole the medical record could perpetrate insurance fraud or prescription fraud. The fraudster could also receive prescriptions to obtain drugs, which could then be sold on the black market. Moreover, the actual victim may be unable to access the medicines that they need because their medical record will reveal that they've already received their prescription in question. Furthermore, the doctor's surgery could risk facing hefty fines, legal proceedings and further criminal and civil charges against them.

It becomes critical, then, that online medical organisations establish identity verification checks in order to create a sophisticated level of trust between the organisation and the patient. This is the only way to ensure that they are dispensing guidance and prescriptions to the real patient on record.

A strong KYP process needs to be watertight at every stage of the process to mitigate these

potentially catastrophic risks. It all begins when a patient opens an online account. Whether it's a GP or a specialist treatment centre, the process starts by requiring the patient to capture a picture of the patient's Government-issued ID (eg driver's license, passport) via the user's smartphone or webcam, and then take a corroborating selfie. During the selfie-taking process, a 3D face map is created to ensure the person behind the ID is the person creating the account. Behind the scenes, the identity verification solution ensures that the ID document is authentic and that the patient pictured in the selfie matches the picture on the ID.

IT WILL COME AS NO SURPRISE THAT THE HEALTHCARE INDUSTRY IS THE MOST BREACHED

The healthcare provider can then check the patient's age to verify that they meet minimum age requirements and confirm through fraud detection analytics that no fraudulent activity has taken place, helping to minimise downstream risk and loss. Based on this information and patient intel, healthcare agencies, including hospitals, offices, clinics and pharmacies, can now approve or deny the new online account.

Moving forward, businesses transitioning into the telemedicine space can continue to verify a patient's identity when they collect online prescriptions and treatments with biometric-based authentication. They do this by capturing a new 3D face map of the patient, comparing it with the original one captured at enrolment to ensure that the patient requesting the prescription is the actual subscriber.

The move away from the vulnerable password-based authentication is absolutely vital in order to prevent opportunistic fraudsters from taking advantage of this growing, and incredibly important, space. Telemedicine has gone mainstream and it's likely to become the new normal because of the convenience it offers to patients. With a strong KYP process in place, telemedicine can realise its full potential without the looming threat of fraud and cybercrime.

The UK has witnessed an overdue, and well-deserved, explosion of gratitude towards its NHS. Whether it was the weekly clap for our carers initiative, or brands offering discounted/free services for NHS staff, we've been reminded of the vital, lifesaving work our medical professionals are doing. Likewise, the expedited modernisation of the healthcare industry and the dramatic shift to telemedicine has undoubtedly supported millions of patients who may not have been able to be adequately treated otherwise.

At a time when the NHS is so stretched, this shift to telemedicine has, and will continue to, play a vital role in the future of healthcare. However, this future is dependent on the ability to reliably establish trust between a medical expert and online patient to avoid cybercriminals taking advantage of this new opportunity. By implementing KYP strategies, we can ensure that telemedicine is not only a short-lived response to the pandemic, but a genuine way of revolutionising healthcare for the future ●

Philipp Pointer, serves as Jumio's Chief Product Officer (CPO) and facilitates Jumio's product strategy. Prior to Jumio, Philipp was responsible for paysafecard, Europe's most popular prepaid solution for purchasing online.

Turning to online medical advice and services has become the norm during the global pandemic