Coronavirus (COVID-19) Resources

Message from Nelson Hardiman:

We are living through a public health crisis as the coronavirus (COVID-19) pandemic spreads across the globe. At Nelson Hardiman, we have been fielding calls nonstop in recent weeks from organizations struggling with emerging issues, including decisions about how to respond to the evolving risks, the need for new policies to address safety challenges, and privacy concerns fueled by a demand for information on infectious disease risks.

Nelson Hardiman is committed to the health and wellbeing of our entire community. We are standing shoulder to shoulder with the healthcare community in responding to the crisis presented by COVID-19. What does that mean?

1. Nelson Hardiman remains open and hard at work. Our team is responding to the needs of healthcare providers –hospitals, telehealth providers, product manufacturers, senior care providers, labs, pharmacies, physician practices, and more – as well as other organizations addressing workforce and health issues. Whatever points of confusion or new questions around COVID-19 you are experiencing, we are here to help.
2. Nelson Hardiman will be sharing content in the coming weeks and months as the situation evolves to provide updates and resources on emerging issues presented by COVID-19. If you have ideas about what you would like to know, we are open to your suggestions. Please email info@nelsonhardiman.com.

3. In the interim, we encourage everyone to regularly visit the Center for Disease Control and Prevention (CDC) Coronavirus resource page for best practices and essential information. We also recommend the World Health Organization (WHO) resources.

We will be providing more information ahead. In this difficult time, we send our prayers for you, your family, friends, and communities to be safe and healthy.

Nelson Hardiman, LLP.

COVID-19 Resources (last updated 4/2/2020)

Our COVID-19 resource page includes federal and state resources on COVID-19 and will be updated over the course of this crisis to keep you informed of the latest developments.

For further information, please contact Harry Nelson at hnelson@nelsonhardiman.com

For media inquiries, please contact Jennifer Coren at jcoren@nelsonhardiman.com

Federal Resources

Coronavirus Preparedness and Response Supplemental Appropriations Act, 2020, Pub. L. 116-123 (3/6/20) (Provides $8.3 billion in emergency funding for federal agencies to respond to COVID-19 outbreak and providing waiver authority for Medicare coverage of telehealth services during certain emergencies).

CMS:

- CMS COVID-19 Partner Toolkit, including link to CMS Landing Page re Current Emergencies, including COVID-19

- CMS Waivers
- CMS COVID-19 FAQs (3/12/20)
- Information for PACE Organizations Regarding Infection Control and Prevention of Coronavirus Disease 2019 (COVID-19) (3/17/20).

Including:

- Information to Medicare Advantage Organizations Related to COVID-19 (3/10/20).
- Dialysis Facilities: QSO-20-19-ESRD, Guidance for Infection Control and Prevention of Coronavirus Disease 2019 (COVID-19) in dialysis facilities (3/10/20).
- Home Health: QSO-20-18-HHA, Guidance for Infection Control and Prevention Concerning Coronavirus Disease 2019 (COVID-19) in Home Health Agencies (HHAs) (3/10/20).
- Respirators: QSO-20-17-ALL, Guidance for use of Certain Industrial Respirators by Health Care Personnel (3/10/20).
- Hospice: QSO-20-16-Hospice, Guidance for Infection Control and Prevention Concerning Coronavirus Disease 2019 (COVID-19) by Hospice Agencies (3/9/20).
- EMTALA: QSO-20-15 Hospital/CAH/EMTALA, Emergency Medical Treatment and Labor Act (EMTALA) Requirements and Implications Related to Coronavirus Disease 2019 (COVID-19) (3/9/20).
- Nursing Homes: QSO-20-14-NH Revised 3/13/20, Guidance for Infection Control and Prevention of Coronavirus Disease 2019 (COVID-19) in nursing homes (revised 3/9/20). CMS Announces New Measures to Protect Nursing Home Residents from COVID-19 (3/13/20).
- Hospitals: QSO-20-13-Hospitals, Guidance for Infection Control and Prevention Concerning Coronavirus Disease (COVID-19): FAQs and Considerations for Patient Triage, Placement and Hospital Discharge (3/4/20).
- QSO-20-12-All, Suspension of Survey Activities (3/4/20)

- QSO-20-10-CLIA, Notification to Surveyors of the Authorization for Emergency Use of the CDC 2019-Novel Coronavirus (2019-nCoV) Real-Time RT-PCR Diagnostic Panel Assay and Guidance for use in CDC Qualified Laboratories (2/6/20).
- QSO-20-09-ALL, Information for Healthcare Facilities Concerning 2019 Novel Coronavirus Illness (2019-nCoV) (2/6/20).

CDC

- CDC Coronavirus 2019 Landing Page
- CDC ICD-10-CM Official Coding Guidelines (2/20/20)

California Resources

California Department of Public Health

- California Department of Public Health Landing Page for Guidance Documents re COVID-19
- Letter to Laboratories – Important information for laboratories about testing for COVID-19 (3/24/20).

Including CDPH All Facilities Letters:

- California Governor's Executive Order Further Enhancing State and Local Government's Ability to Respond to COVID-19 Pandemic (3/12/20).
- Guidance for Limiting the Transmission of COVID-19 in Long-Term Care Facilities (3/11/20).
- Hospitals Surge Survey to Assess Capacity Regarding Coronavirus Disease 2019 (COVID-19) and Reminder to Contact Medical Health Operational Area Coordination Office
- Guidance for Healthcare Facilities on Preparing for Coronavirus Disease 2019 (COVID-19) (3/3/20).
- Infection Control Recommendations for Facilities with Suspect Coronavirus 2019 (COVID-19) Patients (2/28/20)
- Environmental Infection Control for the Coronavirus

Disease 2019 (COVID-19) (2/19/20)

- 2019 Novel Coronavirus Interim Guidance for Risk Assessment and Health Management of Healthcare Personnel with Potential Exposure (2/10/20)
- State Health & Emergency Officials Announce Latest COVID-19 Facts: *New Guidance Issued to Long-Term Care and Adult and Senior Care Facilities, (3/14/20)*
- AFL 20-24. Guidance for Procedures and Transfer of Deceased Persons with Confirmed or Suspected Coronavirus Disease 2019 (3/16/20)

Telehealth Resources

- Telehealth Coverage Policies in the Time of COVID-19 To-Date (3/23/20).
- CMS General Provider Telehealth and Telemedicine Tool Kit (3/20/20).
- California Telehealth Policy – COVID-19 Changes (3/23/20).
- ESRD Provider Telehealth and Telemedicine Tool Kit (3/20/20).
- Office of Civil Rights Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency, including FAQ.
- Medicaid State Plan Fee-for-Service Payments for Services Delivered Via Telehealth (3/17/20).
- Medicare Telemedicine Health Care Fact Sheet (3/17/20).
- Medicare Telehealth Frequently Asked Questions (3/17/20).
- HHS Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency.

Other

- Department of Managed Health Care Memo to All Full Service Commercial and Medi-Cal Health Care Service

Plans re COVID-19 Screening and Testing (3/5/20)

- California Governor's Proclamation of State of Emergency (3/4/20)
- California Employment Development Department COVID-19 Landing Page

---

How the Apple Watch (with a Little Help from AI) Can Save Doctors Time

Electronic health records (EHRs) may be ubiquitous in the healthcare landscape, but that doesn't mean they're necessarily making physicians' lives easier.

Dr. Manish Naik is chief medical information officer at Austin Regional Medical Clinic in central Texas. He told Healthcare IT News that EHRs actually can serve more as obstacles than aids to doctors since they require them to spend a great deal of time, in total, on entering data.

Does typical EHR protocol make doctors "the most highly trained data entry clerks in the world"?

"The user interface is suboptimal and clunky, leading to increased cognitive load," Naik said. "Physicians are acting as the most highly trained data entry clerks in the world to

complete many of their EHR workflows. To cope with these challenges, physicians have begun to bring the EHR into the exam room with their patients, taking focus away from the patient."

Therefore it should be no surprise that Austin Regional – with more than two dozen facilities in ten Texas cities – has been on the hunt for a way to make EHR use more efficient and effective and, at the same time, make way for more focused, hands-on time with patients.

What might be surprising is the device proposed to achieve that result . . . the popular Apple Watch.

Voice recognition program allows doctors to dictate findings into Apple Watch

Artificial Intelligence (AI), machine learning, speech recognition, and natural language processing . . . they're all employed in healthcare vendor Notable Health's tech platform to assist physicians in documenting discussions with patients and seamlessly adding them to EHRs. And the Apple Watch is the vehicle for that delivery system.

"The software assists with physician documentation because the physician can simply dictate their findings into the Apple Watch before, during and after a visit," Naik told Healthcare IT News. "Simply by stating the section that is being dictated, such as 'HPI' or 'physical exam,' the technology places the text in the correct section of the note."

Those worried about AI supplanting human quality control will be reassured to learn that the workflow includes physician review of the AI-generated note; the doctor also will

electronically sign the note in the EHR.

Additionally, Notable Health's technology can be aligned with the practice's specific operating systems. In Austin Regional's case, Notable's tech is integrated with the Epic EHR system used by physicians so that routine workflow – like coding and ordering – is also streamlined and made more efficient.

Because technology of this sort is only as good as its application in real life, the true test comes in its day-to-day usefulness. And so far, six months into the use of AI-via-Apple Watch, Naik gives Notable's technology high marks when it comes to usefulness in the field, both in implementing the technology and in supporting it.

"Incredibly, while the software is integrated on top of our Epic EHR, going live with Notable Health required very little work from our internal IT and EHR teams," Naik said. "At the onset, we certainly were skeptical that the software would be able to integrate so seamlessly with Epic. But Notable Health's team did all of the heavy lifting for us, and we were able to go live within a couple of weeks of signing the contract with them."

Physicians at Austin Regional credit the technology with saving them on average between one and two hours per day, hours they would have otherwise spent on documenting doctor-patient discussions in EHRs.

A reduction in workload means a lower likelihood of physician burnout

Naik explained to Healthcare IT News that that recovered time

adds up in a big way in the lives of doctors. “This improved efficiency has also led to decreased symptoms of burnout from EHR documentation. Physicians have reported that they are able to see more patients throughout the day, focus more on their patients during office visits, and still leave the office earlier to spend more time with their families.”

Obviously this success story has major implications for data collection in the healthcare field at large. Naik warns that doctors often feel overwhelmed by typical EHR platforms. He suggests that providers look into novel methods – including AI – for reducing that burden and thereby reducing burnout . . . a state that doesn’t only impact doctors.

“The effects of these burnout symptoms extend across an organization,” Naik said, “from the clinical staff that works with the MDs to the front desk team to the billing and coding organizations.”

At the present time, over 30 Austin Regional physicians are using the Notable tech platform in their practices: surgeons, orthopedic specialists, family medicine practitioners, rheumatologists, cardiologists, and obstetricians and gynecologists, to name a few. Naik reports that more doctors are joining the AI collaboration each week.

So when you see a physician sporting an Apple Watch, it very well may be that they’re doing more than tracking time: they’re saving it.

Opioid Company Execs Found Guilty of Bribing Docs to Prescribe Drugs

As the country's opioid crisis continues to rage, a recent jury verdict in a federal case illustrates the widening circles of accountability. It may be easy for those untouched by the epidemic to place all the blame squarely on the individuals battling opioid addiction. Increasingly, however, the public is looking to pharmaceutical execs and decision-makers for their part in contributing to the ongoing tragedy.

The latest example of this is the case against Insys Therapeutics, a large opioid company. Executives were accused of offering physicians bribes to prescribe Insys's fentanyl-based pain medication, Subsys, to their patients. And the jury was convinced the allegations were true, charging the company's founder John Kapoor – along with four Insys executives – with criminal racketeering.

Subsys has been approved for pain management in cancer patients, but the case against Insys accused the company of clinging to the goal of high sales no matter what and no matter the patient's actual need.

Executives allegedly provided physicians with incentives to write prescriptions

The *New York Times* reported that prosecutors alleged that Insys used the cover of educational talks that never occurred to dangle bribes in front of doctors (and, in a more salacious allegation, a former employee testified to witnessing one of the company's sales directors, who happened to have experience as an exotic dancer, try to encourage a physician to prescribe Subsys via a "lap dance"). Further, prosecutors accused the company of deceiving insurance companies into paying for the drug under false pretenses.

The Boston federal jury deliberated for 15 days, finding all five executives guilty; they each face the possibility of prison time.

Going after drug companies for irresponsible or illegal practices involving opioids is not new, though judging by the number of cases underway, it does seem that it's becoming a more mainstream approach. Looking back to one of the earliest lawsuits of this sort, Purdue Pharma, the maker of OxyContin, was charged with misleading marketing in 2007. Three of the company's executives were found guilty and sentenced to probation, community service, and over $630 million in fines.

And more recently, just last month federal prosecutors charged the Rochester Drug Cooperative (a large pharmaceutical distribution company) for actions that exacerbated the opioid epidemic, and this month another distributor, the McKesson Corporation, settled the case against it in a West Virginia court with an agreement to pay $37 million in penalties.

Scores of suits are pending as the public seeks to hold drug companies accountable

At the present time, hundreds of lawsuits are pending against drug companies, some that originate at the federal level, some at the state level. Purdue Pharma has recently settled a case brought against it by the state of Oklahoma. And a federal judge in Cleveland has bundled together well over one thousand distinct government lawsuits in order to resolve the cases sooner than if they remained separate.

In the last two decades, the nation’s drug overdose epidemic has claimed more than 700,000 lives. Experts warn that the next decade could see hundreds of thousands more fatalities due to opioids alone if the crisis is left unchecked.

And funding for addiction treatment is one of the most important ways to shift the tides.

Legal action against drug companies not only serves the purpose of putting a stop to illegal behavior that adds fuel to the raging crisis (as it hopefully convinces other companies from even going down that path in the first place), but the monetary settlements can be used to pay for those suffering from substance use disorder to get they help they need, a sector of healthcare that has been consistently underfunded.

Michigan Physicians' Practice Closes Its Doors After Hackers Erase All Data

When patients leave their healthcare provider's office, they may not stop to consider that they're leaving something behind. And yet, sensitive patient data is necessary for the running of the practitioner's business, even as it leaves patients vulnerable to some degree.

According to a report by specialist insurer Beazley that analyzed 2018 cybersecurity data, ransomware attackers target the healthcare industry more than any other. And those attacks are on the rise, with a spike in the final months of last year.

Unless you've been personally affected by a cybersecurity breach or attack, the consequences may sound more abstract than concrete. But a recent case in Michigan illustrates the potentially devastating results of fully executed hacking.

As reported by the news outlet WWMT West Michigan, Brookside Ear, Nose and Throat and Hearing Center will close after cybercriminals wiped out the entirety of the practice's patient files.

Physicians refuse ransom

request; hackers wreak havoc

Ransomware hackers ordered the practice to pay $6,500 to decrypt the IT system’s fully encrypted files. The cybercriminals were met with flat refusal by John Bizon, MD, and William Scalf, MD, the co-owners and co-founders of Brookside ENT and Hearing Center, at which point the hackers completely razed the practice’s digital landscape.

In addition to all of the patient records, all payment data and calendar and scheduling information was deleted. However, Bizon said that because the patient data remained encrypted, the cybercriminals were not able to access that sensitive information to use it for identity theft.

Faced with the daunting task of piecing the practice back together without a shred of information to get them going, Bizon and Scalf opted to retire from medicine ahead of schedule instead. Understandably, that’s not a decision that sits well with all patients.

A patient spoke with WWMT and reported finding out about the file erasure when she called the office to schedule a post-surgery follow-up visit. Because the exact details of that particular surgery were contained in the now-deleted Brookside’s records, the patient’s new provider will not have the benefit of that medical history going forward. So although her data was not compromised in a way that leaves her open to what we typically fear after a breach (thanks to the encrypted files), she faces unanticipated hurdles involving her future care, through no fault of her own.

The cybercriminals have not yet been apprehended, although the FBI is presently investigating the incident. Brookside’s owners have said that they believe the ransomeware attack was limited to their practice.

Smaller practices seem particularly vulnerable

When it comes to ransomware attacks, cybercriminals prefer practices like Brookside ENT and Hearing Center – in other words, small-to-medium organizations, which are the subject of these types of attacks more than 70% of the time. And that's no accident.

"Unfortunately, it's often smaller businesses that are most vulnerable to attack by cybercriminals as they frequently lack the resources and protocols of larger firms," Beazley Breach Response Services Head Katherine Keefe told HealthITSecurity when the report was released. "Businesses of all sizes need to ensure their IT employees are aware of the risks through up-to-date training and implementation of cyber security measures."

Education is the key to prevention

Beazley reported that although accidental disclosure leading to data breaches dropped by more than 10% over the previous year, it still represented the most common cause of cyber-vulnerability. Malware and hacking jumped from 20% to 30% over the period of one year.

Naturally, cyber-attacks are not exclusive to healthcare; the report revealed that events involving compromised business emails spiked dramatically in 2018, and those attacks ensnared healthcare, finance, education, and various professional services.

In a statement following another cybersecurity report, Keefe

said: “Unfortunately, we see these threats globally across all sectors, and we strongly believe that education about the risks and preparedness are as important as IT security measures for protecting individuals and assets from cyberattacks.”

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

Risky Business? OIG Finds Room for Improvement in NIH’s Data Sharing

Earlier this month, the National Institutes of Health (NIH) received the results of an audit by the Department of Health and Human Services’ Office of the Inspector General (OIG). The agency’s findings included concern over risks in NIH data sharing processes, despite the fact that NIH itself disputed some of those OIG conclusions.

The audit specifically sought to assess whether the NIH was sufficiently protecting sensitive data when it was shared. The OIG’s assessment lens was established Federal guidance, and the agency also interviewed NIH employees to reach its determination.

NIH is urged to bring in outside experts

Ultimately, the OIG concluded that NIH's controls regarding data access permissions and monitoring are not fully adequate for those critical tasks. The OIG furnished NIH with specific suggestions for strengthening those data access controls, and also urged the agency to seek help from a firm outside the government that has experience with ameliorating the misuse of scientific data.

"NIH could strengthen its controls by developing a security framework, conducting a risk assessment, and implementing additional appropriate security controls designed to safeguard sensitive data," the OIG's report stated.

Although the OIG did not share the specific data control risks it found with the public, the statement went on to say, "We also recommend that NIH develop and implement mechanisms to ensure data security policies keep current with emerging threats. . . [W]e recommend that NIH make security awareness training and security plans a requirement."

NIH rejects some of the audit's conclusions

However emphatic the tone of the OIG's findings, NIH officials did not accept them all as fact, according to the OIG. Specifically, the NIH pushed back when it came to the OIG suggesting the implementation of new data controls, the carrying out of a risk assessment, the creation of a security framework, and new controls to guarantee training and security plan mandates.

Where the two agencies saw eye to eye was in the matter of the need for NIH's policies to change according to changes in the types of threats to sensitive data. Further, NIH officials reported the development of a group tasked with decreasing security risks to intellectual property as well as the protection of the fruits of peer review processes.

Acknowledging NIH's refutation of parts of the OIG's findings, the latter doubled down on its conclusions (calling them "valid") and urged the biomedical research agency to remain open to ways of evaluating and addressing issues highlighted in the report.

"We recognize that NIH reported that it is already taking certain actions, such as the working group that was recently established, that may address our recommendations," OIG officials said. "If NIH determines that it does not need to strengthen its controls, it should document that determination consistent with applicable Federal regulations and guidance."

According to the OIG, "NIH is the largest public funder of biomedical research agency in the world, investing more than $30 billion in taxpayer dollars to achieve its mission. NIH's mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability."

Cash-only Still Burdening Legal Cannabis Businesses

The legal cannabis industry here in the Golden State and in the more than two dozen other states where it's sanctioned (not to mention our neighbor to the north where it's legal countrywide) promises big profits. You'd be hard-pressed to find an aspiring cannapreneur unaware of the potential bottom line. But here's the rub: the greater the profit, the greater the headache for the majority of legal marijuana businesses. Aside from the product itself, the one thing illicit and legal cannabis ventures have in common? They're both cash-only operations.

In an undeniably electronic age, it may seem archaic to rely on paper money. Indeed, it's becoming more common for retail establishments outside of the cannabis industry to do away with cash sales altogether. Not only is a cashless business far safer ("no cash on premises" is much more of a robbery deterrent than "employee doesn't have combination to safe"), but it's also far more efficient from an accounting standpoint, and it's less costly, too (hiring armed drivers to transport and guard the spoils ends up taking a bigger bite out of a business than banking fees would).

None of those pragmatic arguments on their own have the power to change the federal law, however, which still classifies marijuana as a Schedule I drug, alongside substances like heroin and Ecstasy. Because banks operate under federal mandates, they aren't keen to wade through the murky gray area posed by state-legal money pulled in by a federally-illegal product . . . even when that money is estimated to be $5 billion per year, the projection for California's cannabis transactions alone.

Marijuana businesses should prepare to wait . . . and wait . . . and wait

There are a few exceptions, though – very few. At present there are only five financial institutions in the state willing to work with marijuana businesses. All are credit unions, including one in Santa Rosa and one in Santa Cruz. However, if cannapreneurs are interested in parking their cash in one of those credit unions, they won't get further than the end of a long waiting list: none are taking on new clients, and the financial institutions themselves are loath to talk about the marijuana businesses they currently service, making it hard for business owners to learn from example.

Marijuana businesspeople might not be hand-wringing over the thorny liability of piles of cash had the 2016 presidential election had gone another way.

In addition to granting state-compliant legal marijuana businesses some degree of reassurance that the U.S. Department of Justice (DOJ) would not use its resources to prosecute state-legal operations, the Cole Memo, issued during the Obama administration, also extended some peace of mind to financial depositories wishing to work with legal canna-businesses. Among other controls, banks were required to conduct regular audits and report on the movement of marijuana money.

However, former U.S. Attorney General Jeff Sessions, appointed by Donald Trump, rescinded the Cole Memo, and along with it, banks' tenuous peace of mind when it comes to dealing with marijuana operations. At this moment, it's anyone's guess whether William Barr, the new AG, will reinstate the Cole Memo or afford legal marijuana businesses similar reassurances. The current legal federal climate is such that banks backing

marijuana businesses run the risk of being investigated for money laundering or being prosecuted for facilitating an illegal business.

It’s no wonder most traditional banks, plenty profitable without getting anywhere near marijuana, are choosing to stay away.

California has explored the possibility of developing its own financial institution in order to open its doors to canna-cashflow, but it seems like it holds a slim chance of actually happening. The state treasurer released a report at the close of 2018 projecting a substantial loss for the state should it attempt such a feat. It would require $1 billion in investments at the outset, and would be further challenged by a bevy of federal snags should it get that far.

Is there even a whiff of optimism?

Legal marijuana is a growing business, in more ways than one. Although what to do with all that cash presents an incredibly onerous dilemma for many people active in the industry here at home, it’s hard to imagine that it will stay that way in the long run.

According to data released by the U.S. Department of Treasury’s Financial Crimes Enforcement Network in the autumn of 2018, across the country, there are nearly 500 financial institutions extending a hand to cannaprenuers. (Around four-fifths of those are traditional banks and one-fifth credit unions.) That’s up from around 100 five years ago. The majority of those institutions limit their transactions to local cannabis operations.

Despite California’s relatively and dramatically limited

options for banking, some industry insiders believe the landscape is likely to grow a bit more lush in the coming year. For instance: Tyler Beuerlein of Hypur, an Arizona-based company that provides banking technology to cash-centric businesses like those in the legal marijuana industry. Beuerlein told *The Mercury News* that he believes that 2019 will see new banking options crop up for California canna-businesses . . . which means that in addition to vigilance in the meantime, business owners will need to strive for patience too.

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

Investigation into $20M Healthcare Fraud Scheme Ends with Conviction of Doctor, Hospital Owner

The U.S. Department of Justice (DOJ) has long maintained that one of its top priorities is to quash healthcare fraud. Ongoing investigations and trials indicate the government's commitment to that goal, and a recent conviction by a federal jury in Houston speaks to that.

As announced in a DOJ press release, Dr. Harcharan Narang, 50, and hospital owner Dayakar Moparty, 47, were recently

convicted of conspiracy to commit healthcare fraud, 17 counts of healthcare fraud, and three counts of money laundering. The jury returned its verdict after a two-week trial and after four hours of deliberation. The FBI and the Office of Personnel Management, Office of Inspector General conducted the investigation.

Narang, an internal medicine doctor who owned North Cypress Clinical Associates in Houston, and Moparty, who managed Red Oak Hospital in Houston, allegedly conspired to defraud the government out of $20 million. The jury was presented with evidence over the course of the trial alleging that Narang and Moparty submitted false and fraudulent claims for tests that were not medically necessary and/or were not provided to the patients. Further, they allegedly billed for those services at a higher reimbursement rate at Red Oak Hospital.

Patients say they were lured in with Groupon, then hit with a string of tests

Allegedly, Moparty told his staff to falsely bill certain medical services at Red Oak Hospital that were not actually delivered. And Narang (along with co-conspirators) allegedly spun some fiction on home health patient assessment forms in order to make patients seem sicker than they were in truth, with the goal of billing for those services at higher reimbursement rates. Aetna, Blue Cross Blue Shield, and Cigna were some of the insurers in receipt of those falsified documents discussed during the trial.

The trial also included testimony by patients stating that they thought they had purchased a Groupon for weight loss shots. Despite what got them in the door, they ultimately underwent a series of medical tests that were allegedly not

needed and/or not provided, this after meeting Narang. Red Oak Hospital received around $3.2 million from healthcare benefit programs. The alleged scheme perpetrated by Narang and Moparty had the latter secretly paying the former around $3 million and hiding that money by spreading it around various corporations owned by Narang.

Doctor and hospital owner face decades in prison

Both men face up to a decade in federal prison for each count of healthcare fraud, as well as 20 years for each count of money laundering. Their sentencing is set for late June (before U.S. District Judge Sim Lake); they are currently out on bond and monitored with ankle devices.

Narang and Moparty allegedly conspired with Dr. Gurnaib Sidhu, 67, of Houston, who is awaiting sentencing after pleading guilty to conspiracy to commit healthcare fraud.

Cybersecurity Check-In: New

Study Reveals Phishing Attempts Soared in 2018

With the new year well underway, it’s a good time for healthcare providers to look back on 2018 to determine patterns of cybersecurity attacks and better cyber-strategize for the year ahead.

Proofpoint researchers recently released a new study that reveals that phishing attacks were dramatically on the rise last year, and the hackers’ overwhelming focus: credential compromise. This type of attack surged by more than 70% over 2017, beyond even malware infections. Credential phishing attacks were noted by 65% of the infosec professionals participating in the study, whereas only 38% of participants reported that kind of attack in 2017. Malware attacks remained steady at just under 50% for both 2017 and 2018.

Credential compromise: a “dangerous trend”

The authors of the report noted that phishing emails of this sort represent a “dangerous trend given the serious ramifications of a successful credential compromise attack… This is of particular concern given that multiple services often sit behind a single password.”

The Proofpoint project surveyed 15,000 infosec professionals from across the globe and across industries, and it also studied millions of phishing emails sent between October and September of 2018. The researchers determined that 83% of survey participants had been the target of phishing schemes, as opposed to 73% for 2017.

“More respondents said they experienced attacks during 2018 than in 2017,” the study’s authors wrote. “Phishing and spear phishing saw the biggest increases, but all types of attacks happened more frequently than in 2017.”

The healthcare industry didn’t get the worst report card grades, but there’s much room for improvement

Healthcare cybersecurity is of the utmost importance considering the level of sensitivity of patient data, but that doesn’t mean IT professionals’ best efforts can prevent all attacks. For instance, 2018 saw the New York Oncology Hematology breach, in which 15 staff members failed to recognize the phishing attack for what it was, and ultimately, the data of 128,000 individuals (patients and employees) was compromised.

However, when compared with other industries, healthcare’s cybersecurity prognosis was nowhere near the worst. The report determined that healthcare’s “average failure rate” was 8%. This compared to the entertainment industry, which suffered a failure rate exactly double that at 16%. When it came to the click-through rate for malicious links embedded in phishing emails that send the victim to a page to enter their personal data, however, the healthcare sector came in at 13%.

Those malicious links, used in nearly 70% of all attacks, are the most common type of phishing attempt, according to the Proofpoint researchers. Only 17% of phishing campaigns employed a direct data form for collecting victims’ personal information rather than a link sending them to another page, and 14% of phishing attempts use malicious email attachments

to try to steal data.

Before you click that link . . .

Among the types of schemes that most commonly compelled victims to enter their personal information were emails that alerted users to password changes, invoice payments, toll violations, and new building evacuation plans.

“Across the board, infosec professionals identified a more active social engineering landscape in 2018,” the report authors wrote. “The vast majority—96%—said the rate of phishing attacks either increased or stayed consistent throughout the year.”

Nearly all professionals surveyed are training users in anti-phishing security

The news isn’t all bleak, however; the study included a promising statistic: 95% of infosec professionals reported training end users on identifying and avoiding phishing campaigns. Further, the majority of the survey respondents said they already use threat monitoring platforms, URL rewriting, and spam filters in the ongoing effort to boost cybersecurity and be proactive.

“They are also shifting to a more people-centric model by proactively identifying phishing susceptibility, measuring end-user risk, and delivering regular security awareness training,” the Proofpoint researchers stated.

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

New Report Sees Digital Therapeutics as "Reshaping the Landscape" of Certain Aspects of Healthcare

"Top health industry issues of 2019: The New Health Economy comes of age" is the title of the recently released report by consulting firm PwC's Health Research Institute. The publication highlights key issues relevant to the healthcare industry as a whole, including tax reform, the Affordable Care Act, and digital health.

PwC's researchers predict that the coming year will usher in new digital therapies that, among other benefits, can provide healthcare practitioners with real-time data, assist patients in making health-positive changes, and improve employers' and insurers' management protocol when it comes to the health of their beneficiaries.

Change is afoot: data sharing

and payment collections

“The arrival of digital therapeutics – an emerging health discipline that uses technology to augment or even replace active drugs in disease treatment – is reshaping the landscape for new medicines, product reimbursement and regulatory oversight,” the report reads. “This means that new data sharing processes and payment models will be established to integrate these products into the broader treatment arsenal and regulatory structure for drug and device approvals.”

PwC noted that 2017 and 2018 saw a hefty $12.5 billion directed to digital health ventures by investors. When held up alongside the year 2013, that more recent investment total is an upswing of 230%. And the size of the average investment deal increased by 67% from 2013 to 2017-18.

“Unlike branded companion apps and online portals, digital therapeutics and connected devices are clinically validated by the FDA and target specific health outcomes,” PwC said. “The FDA already has approved some new digital therapies, such as Boston-based Pear Therapeutics’ Reset mobile application for the treatment of substance abuse, and Stockholm, Sweden-based Natural Cycles’ birth control app.”

Digital devices often work alongside drugs, not instead of drugs

Another prediction contained within the report: the emergence of digital devices intended to treat chronic medical conditions such as diabetes and disorders of the central nervous system, and some of those connected devices, rather than supplanting the need for pharmaceuticals, will complement

them.

And when it comes to digital devices and how they can work within connected care in the life sciences field, the PwC offered three pieces of advice for life sciences organizations: concentrate on outcomes more than endpoints; assess how digital therapeutics within connected care affect providers' practices; and seek out partnership prototypes that home in on demonstrable results.

"To succeed in the digital therapeutics era, pharmaceutical and life sciences companies must venture more deeply into care delivery," PwC stated. "Organizations that can become an integral part of giving patients positive health outcomes – using real-world data and enhancing the connection between patients and providers – also will be able to design new payment and contracting models."

The report's authors opined that patients may experience visits to their physicians as more efficient and more useful when new patient data is successfully integrated into healthcare practices, rather than detract from patient-doctor consultation time.

"New health data streams coming in from patients' devices and mobile phones may disrupt provider practices even as they help improve care delivery," PwC said. "Evaluate workflow processes for new data streams, including integration in electronic medical health records."

Efficiency: one of the top goals in new partnership model

An example of the results-driven partnership model is

Innovation Health, an insurer developed by insurance giant Aetna and Virginia-based Inova Health System. Innovation Health is currently putting digital therapeutics and financial models to the test to determine the efficacy of new products.

“Digital therapeutics and connected devices may make it easier to construct value-based contracts and other outcomes-based financial models with payers and providers to drive adoption,” PwC stated. “Subscription pricing for digital therapeutics or connected device solutions, for example, could make pharmacy spending more predictable and efficient.”

Pathology Lab Agrees to Pay $63.5M to Settle Illicit Kickback Allegations

The Department of Health and Human Services’ Office of Inspector General (OIG) recently announced a settlement reached in a False Claims Act case involving a pathology laboratory. And, as always, healthcare professionals are wise to take notice of the government’s seriousness in approaching allegations of fraud.

Before company ownership changed hands in 2017, the Irvine, Texas-based Inform Diagnostics operated as Miraca Life

Sciences Inc., a subsidiary of the Japanese company Miraca Holdings Inc. The company was the subject of three *qui tam* actions that alleged Inform/Miraca participated in financial entanglements that violated the Anti-Kickback Statute and the Stark Law. In order to resolve those allegations, the company has agreed to pay $63.5 million.

DOJ warns that kickbacks "can alter a physician's judgment"

"The Department of Justice has longstanding concerns about improper financial relationships between health care providers and their referral sources because those relationships can alter a physician's judgment about the patient's true health care needs and drive up health care costs for everybody," said Assistant Attorney General Jody Hunt of the Department of Justice's Civil Division in an OIG press release. "In addition to yielding a substantial recovery for taxpayers, this settlement should deter similar conduct in the future and help make health care more affordable."

Allegedly, Inform Diagnostics/Miraca Life Sciences subsidized electronic health records (EHR) systems for referring physicians, as well as lower cost (or no-cost) tech consulting services, thereby violating the federal Anti-Kickback Statute and the Stark Law, which limit the types of financial arrangements healthcare providers may transact with physicians who send patients their way. Labs are not exempt from these restrictions.

Fraud enforcement as an

ongoing effort: “We will continue to enforce the laws . . .”

The OIG’s press release on the matter includes this statement by U.S. Attorney Don Cochran of the Middle District of Tennessee: “The wellbeing and needs of the patient should always be a medical provider’s primary considerations. The restrictions imposed by federal statutes exist to prevent improper influence on the parties prescribing and providing medical services, including laboratory tests. We will continue to enforce the laws that protect the integrity of federal health care programs.”

The case against Inform Diagnostics/Miraca Holdings was investigated by the Civil Division’s Commercial Litigation Branch, the U.S. Attorney’s Office for the Middle District of Tennessee, the U.S. Attorney’s Office for the Middle District of Florida, the Department of Health and Human Services Office of Inspector General, and the FBI. Although the settlement resolves the matter, it is not an admission of guilt on the company’s part; the allegations remain just that.

And although on the surface it looks like the government and the whistleblowers are the parties benefitting from the resolution of the case, it’s true that the public benefits when physicians aren’t making referral decisions based on illegal inducements.

“When health care providers are distracted by suspect financial arrangements, the interests of patients can be cast aside,” said Special Agent in Charge Derrick L. Jackson of HHS OIG. “Our agency, working closely with our law enforcement partners, will continue to protect patients and the federal health care programs that serve them.”

U.S. Attorney sees this action as “commitment” to fight healthcare fraud

“Patients deserve the unfettered, independent judgment of their health care professionals. Offering financial incentives to physicians and medical practices in exchange for referrals undermines citizens’ trust in our health care system,” said United States Attorney Maria Chapa Lopez of the Middle District of Florida. “With this settlement, our Civil Division confirms its commitment to our nation’s critical struggle against practices that put public health programs at risk.”

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

FDA Seeks to Curb Opioid Deaths by Making Overdose Drug Naloxone OTC

Despite heightened collective awareness, the opioid epidemic in this country continues to rage without improvement. Quite the contrary, a new report by the National Safety Council shows that the lifetime odds of accidental death due to an opioid overdose in the U.S. have now surpassed the odds of

dying in a motor vehicle accident. This is the first time that opioid fatalities (1 in 96) have edged out auto fatalities (1 in 103) on the list. As in previous years, opioid-related death is more likely than death involving fire or falls or drowning or pedestrian events. Only the odds of suicide (1 in 88) are still higher than opioid overdose.

According to the Centers for Disease Control and Prevention (CDC), more than 70,000 deaths in the nation in 2017 (the same year of the Safety Council's study) were attributed to drug overdose (48,000 due to opioids, both prescription and illicit). And the CDC pointed to illegally manufactured fentanyl as the reason for the surge (63,600 people died due to drug overdose in 2016).

FDA head explains the agency's effort in statement

Dr. Scott Gottlieb, the Commissioner of the U.S. Food and Drug Administration (FDA), recently released a statement that speaks to what he calls an "unprecedented" move toward providing some relief for the incredibly dire national crisis of opioid-related deaths.

Gottlieb has announced the FDA's plan to make naloxone (a drug used in the prevention of opioid overdose and currently only available with a prescription) more readily and widely accessible by making it an over-the-counter medication (OTC). Naloxone is used to counter the effects of opioid overdose, but it must be administered rapidly if it is to reverse the loss of consciousness and breathing associated with dangerous opioid levels. In his statement, Gottlieb opined that the stigma of substance abuse disorder may dissuade many individuals from seeking a doctor's care, thereby putting up a major obstacle between naloxone and the people who most need to have it on hand.

The FDA Commissioner went on to explain that for naloxone to go from prescription to OTC would require a change in labeling. For now, the prescribed version is given to the patient with usage instructions on the label, but not with Drug Facts labeling (DFL), a requirement for OTC medications. And in order for a product to earn that DFL, drug companies are required to conduct studies and ultimately demonstrate that the public will be able to use the product as it is intended and without the assistance of a physician. And specifically, OTC naloxone's labeling must be clear enough that an "untrained bystander" would be able to administer it to a patient in an emergency.

"Some stakeholders have identified the requirement to perform these studies as a barrier to the development of OTC naloxone products," Gottlieb wrote in his statement.

FDA developed pictograms to educate public on naloxone use

The FDA has found a potential way around that, according to Gottlieb . . . what he calls an "unprecedented step": simple pictorial representations that demonstrate how the drug should be used.

"This is the first time the FDA has proactively developed and tested a DFL for a drug to support the development of an OTC product," Gottlieb's statement announced. "[W]e've crafted model labeling that sponsors can use to obtain approval for OTC naloxone and increase its access."

The FDA statement is embedded with links to model DFL's for OTC naloxone, one that depicts instructions for using an auto-injector and the other for the nasal spray option.

Gottlieb's statement was released during the partial government shutdown, and he addressed that fiscal backdrop as well: "During this period without a FY19 appropriation for the FDA, we've been focused on making sure that we continue critical aspects of our work, to the extent permitted by law." He went on to explain that the review of applications of certain products (including naloxone) are paid for by "limited carryover user fee balances."

Study of new DFL shows strong consumer comprehension

The FDA reported that the DFL has been tested for consumer comprehension by an independent contractor. The study used more than 700 participants ranging from people actively using prescription opioids or heroin, as well as those with loved ones using opioids, and the general public too. The agency reviewed the final report of that study and "determined that the comprehension results were satisfactory" and that the majority of participants understood the proposed OTC instructional labeling.

"I personally urge companies to take notice of this pathway that the FDA has opened for them and come to the Agency with applications as soon as possible," Gottlieb wrote.

Of course, naloxone can not on its own change the course of the nation's opioid tragedy, as Gottlieb pointed out, but it *can* save lives. He reminded the public that his agency is also working on preventative measures, like better pain management and greater access to treatment for those struggling with substance use disorder.

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should

consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.

Healthcare Cybersecurity: Can Artificial Intelligence Provide a Real Solution?

In 2017, the Health Care Industry Cybersecurity Task Force released a report on cybersecurity in healthcare, and it's not a stretch to say that the prognosis was poor.

Included in the report was the revelation that 75% of hospitals lack permanent, full-time security leaders, compelling some providers to try the less-than-ideal fix of asking other health entities to loan them their security personnel to act as part-time security officers. Additionally, 75% of providers participating in a recent Ponemon report stated that their IT security teams are not adequately staffed, and, exacerbating the problem, they have trouble finding qualified people to fill the vacant positions.

Perhaps this shortage of staff wouldn't be such a dire issue if cybersecurity breaches and attacks weren't ongoing and pervasive, but they are. And that urgent backdrop has some industry experts opining that perhaps the solution isn't in finding more people to do the jobs, but rather, whether artificial intelligence can shore up the vulnerabilities in the healthcare cybersecurity landscape.

“Automation doesn’t mean the elimination of people…”

David Finn is the Vice President of Strategic Innovation for CynergisTek. He explained to Health IT Security that using machine learning or other types of artificial intelligence (AI) can streamline complex, predictable processes such as password criteria (i.e., length and format), password resets, and applying updates and patches.

“In the ‘old’ days this was a very labor-intensive issue: You had to talk to a human being,” Finn said. “Today, because we can identify and authenticate a user and/or device, password resets can be accomplished online, at any time, without a call and without having to tie up another person who may be dealing with a user who is having issues with their computer or an application they’ve never used before.”

However, Finn also added that automating certain processes doesn’t mean that it’s human hands-off for good. Quite the contrary: AI depends upon human attention – both well-defined cyber-protocol at the outset and interactive oversight over the long haul.

Otherwise, without security leaders who set up definitive IT rules and outcomes, Finn warned that “automation efforts may result in more chaos, more work, bigger issues and perhaps less security. You also need to have defined steps for when the process ‘breaks.’ We’ve all been frustrated when we can’t get something done and there is no person to talk to.”

Finn further reminded us via that Health IT Security interview: “Automation doesn’t mean the elimination of people, it means the re-deployment of people to do the work that can’t be automated – work that requires real-time decision-making outside of the prescribed rules.”

Despite low confidence now, SOAR will be spreading in the near future

Indeed, results from the Ponemon report echo Finn's words. Just over three-quarters of the providers participating in the study said that automation may actually be widening the security skills gap in that AI services require more highly skilled security staff, not less, which exacerbates the staffing issue.

Also from that report, just over one-quarter of healthcare organizations reported employing AI as an aspect of cybersecurity. And even less than that – a mere 15% – are even sold on automation at all, saying that they believe that AI should be relied upon and trusted for cybersecurity . . . which means that a whopping 85% don't see AI tools as a solution to the problem of vulnerable healthcare data. However, perhaps surprisingly in light of that statistic, just over 40% of providers say the insufficient number of specialized, highly trained workforce have compelled them to invest in some form of AI for cybersecurity for the future.

Outside of fanciful sci-fi, AI isn't in line to replace people. But security experts believe it can help in the fight against security threats and attacks. A recently-released Gartner report found that by 2020, 15% of healthcare organizations employing five or more security personnel will implement the SOAR program (Security Orchestration, Automation and Response).

The report cited a spike in security alarms and not enough staff to handle them as the impetus for that projected adoption of the SOAR protocol. As it stands now, security teams must manually review large amounts of security data and

gather threat information, an incredibly time-consuming, painstaking process that, without sufficient manpower to carry it out, results in healthcare entities all too often being one step behind the bad actors.

This article is provided for educational purposes only and is not offered as, and should not be relied on as, legal advice. Any individual or entity reading this information should consult an attorney for their particular situation. For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.