THE CONTINUED INTERNATIONALIZATION OF HEALTHCARE: A NEW LEGAL PARADIGM

By: Brett W. Johnson and Claudia Stedman

The on-going COVID-19 pandemic crisis has highlighted the reality that, like all other industries, the provision of healthcare is now almost completely reliant on an international supply chain of both services and product. Domestically, healthcare is more highly regulated at every level of government than any other industry, including the famed military-industrial complex that primarily is only regulated at the federal level. With such a historically heavily regulated industry at the domestic level, the impacts of international trade, which usually rely on flexibility and "just in time" delivery principles, are at times difficult to synchronize or fully appreciate the multitude of legal impacts on a transaction, whether that be the direct providing of healthcare services or supplying the mammoth industry to enable the providing of such services. As a "new normal" related to international trade and the healthcare industry is established, concentration on novel legal issues is important to avoid the sometimes-harsh consequences when domestic regulatory agencies exercise historical oversight.

I. Telemedicine

As the world grapples with the COVID-19 pandemic, the use of telemedicine, or telehealth, has become a popular tool for patients who must abide by social distancing requirements but who still need care. Telemedicine is the use of telecommunication and other information technologies in order to provide clinical healthcare at a distance. In the modern era, this regularly includes cross-border consultations or even remote procedure, which utilize robotic instrumentation. Telemedicine "holds great potential for reducing the variability of diagnoses as well as improving clinical management and delivery of healthcare services worldwide by enhancing access, efficiency, and cost-effectiveness."[1] The most significant gains are seen among typically underserved populations, notably those in rural communities. For all its successes, however, telemedicine may not be the silver bullet that some hope. From an international standpoint, cultural differences, credentialing, compliance with the applicable "community standard of care," and adherence to healthcare facilities' policies and procedures pose significant hurdles to practitioners and patients alike.

A. Cultural Differences

One of the most obvious hurdles for healthcare professionals and patients teleconferencing is not directly a "legal issue," but rather are cultural miscommunications that can lead to significant liability. A major issue arises from language differences and the availability, or lack thereof, of translators. In addition, medical professionals from industrialized communities may not understand the infrastructure (both physical and social) from which their patients are seeking care.

[1] *See* World Health Organization, *Telemedicine: Opportunities and developments in Member States*, 2 REP. ON THE SECOND GLOB. SURV. ON EHEALTH, 11 (2010).

For instance, a lack of "computer literate workers," availability of healthcare staff to assist patients on site with technological difficulties, and gender norms between patients and practitioners can significantly affect access and quality of care.[2] Availability of equipment, supplies, and medicines once a diagnosis has been made has to be considered in the context of the regions where a patient lives and the ease with which he or she can obtain necessary follow-up. The presence or absence of national policy agendas that either include or exclude telemedicine as a means of accessing healthcare likewise has a profound effect on both intra- and inter-border communication between patients and their doctors.

In addition to the traditional international trade terms that are applicable to any agreement for services on an international level (and that are quite different than a domestic transaction), it is important that any agreement to provide such services address cultural realities and have mechanisms to handle communication effectively. Specifically, regardless of whether the practitioner is based on the United States and is providing services in a foreign country, or vice versa, the practitioner should not operate in a silo. A practitioner who can physically still "lay hands" on a patient may be necessary to be a part of the medical team to ensure appropriate care. Policies and procedures, especially those dealing with employee training related to sexual harassment and other appropriate conduct, should be reinforced. For foreign doctors emigrating to the United States, it may be appropriate to include a chaperone for a period of time to overcome any cultural issues.

The more difficult issue are the ancillary practices that may not directly involve "hands on" medical care. For example, radiologists are now based around the world and regularly review images and then provide a written report. The ability for a treating practitioner to fully rely on those remote services without quick communication may lead to repeat images. As referenced, these communications could be hampered due to cultural differences or language barriers. This has multiple "legal" consequences associated with timing of care, medical necessity for the multiple images (and readings), and other supervision issues.

In the United States, practitioners and counsel should check with their state-specific guidelines in order to ensure compliance with licensing and location requirements as many of these provisions have changed as a result of the COVID-19 emergency. For instance, before the pandemic, in Arizona, physicians who "read and/or interpret[ed] medical records and radiology films" had to hold an Arizona license unless that doctor engaged in only a "single or infrequent consultation with" a doctor licensed in Arizona and if the "consultation regards a specific patient or patients."[3]

However, Governor Ducey's March Executive Order has altered these licensing requirements such that any Arizona licensed medical professional can provide telemedicine services regardless of what their licensing board regulations provide. Additionally, practitioners who have prescribing authority are permitted to prescribe medication without first requiring an in-person examination.[4] Additionally, Arizona Senate Bill 1089 has added "asynchronous store-and-

[2] *Id*. at 19.
[3] A.R.S § 32-1421(B)(1) (2020).
[4] *See generally*, Ariz. Exec. Order No. 2020-15 (Mar. 25, 2020), https://azgovernor.gov/sites/default/files/eo_2020-15_expansion_of_telemedicine_0.pdf,

forward technologies and remote patient monitoring technologies, for the purpose of diagnosis, consultation or treatment" to the definition of telemedicine practice.[5]

Many agreements ignore these "real issues" of cross-border telemedicine and attempt to apply a domestic risk shifting tactic utilizing intermediaries to work through such issues. Instead, the communication and cultural issues should be addressed up front in the agreement or accompanying protocols. Further, along with the credentialing process discussed below, healthcare facilities should consider mandated training to address cross-border services and provide mechanisms to resolve any issues to avoid cultural misunderstandings becoming legal liabilities.

B. Credentialing & Privileging

1. United States

While a distant site provider will not have the same privileges with a healthcare facility as an onsite provider, it is imperative that those responsible for credentialing and privileging ensure that the foreign telehealth practitioner is legally allowed to provide the type and scope of care for the particular patient population he or she serves. In the United States, the Centers for Medicare & Medicaid Services ("CMS") "requires each hospital to have a credentialing and privileging process for all practitioners providing services to its patients."[6]

The process as applied to distant site providers, known as "credentialing by proxy," permits hospitals and critical access sites to provide telemedicine services "to their patients through written agreements with a distant-site hospital or a distant-site telemedicine entity."[7] Still, it is important for providers *and* facilities to be aware of the different licensing and credentialing requirements as set forth by the state(s) in which they hold a license(s) and the federal government.

For instance, in the past, CMS rules required telehealth practitioners to be physically located within the United States to treat patients for Medicare-covered services. However, on December 1, 2020, CMS issued "Emergency Declaration Blanket Waivers for Health Care Providers."[8] This declaration permits physicians "whose privileges will expire to continue practicing," allows for "telemedicine services to be furnished to the hospital's patients through an agreement with an off-site hospital," and waives the requirement that doctors be physically located in a Critical Access Hospital (CAH) to "provide medical direction, consultation, and supervision for the services provided . . .."[9]

---

[5] S.B 1089 2019 Leg. 54th Sess. (Ariz. 2019).
[6] Georgia Partnership for Telehealth, *Credentialing By Proxy*, GEORGIA PARTNERSHIP FOR TELEHEALTH (2019), https://gpth.org/wp-content/uploads/2019/04/Credentialing-By-Proxy.pdf.
[7] Director of Survey and Certification Group, *Telemedicine Services in Hospitals and Critical Access Hospitals (CAHs)*, DEPARTMENT OF HEALTH & HUMAN SERVICES, https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/downloads/SCLetter11_32.pdf (last visited, Jan. 24, 2021).
[8] CMS, *COVID-19 Emergency Declaration Blanket Waivers for Health Care Providers*, Centers for Medicare & Medicaid Services, https://www.cms.gov/files/document/summary-covid-19-emergency-declaration-waivers.pdf (last visited, Jan. 24, 2021).
[9] *Id*. at 4-5.

On a state level, physicians may be able to gain privileges if a state in which they wish to practice is a signatory to the Interstate Medical Licensure Compact. This intrastate agreement has become a vital legal tool during COVID-19 to allow practitioners to cross state lines to provide treatment to patients.

Arizona is one such jurisdiction, and permits physicians who hold a "full, unrestricted medical license in a Compact member-state" to practice telemedicine here under certain conditions.[10] Arizona also has universal recognition of licensure, provided the physician has an active license in another state for at least one year and is a resident of Arizona. Many states have eased their licensure requirements for the practice of telemedicine in the wake of COVID-19 and have expanded the list of licensed medical professionals who can provide telehealth services.

However, it cannot be assumed that the practitioner is properly credentialed. Healthcare facilities that utilize such out-of-state services must still review and document that the practitioner providing remote services is properly credentialed and meet the skill requirements to meet the applicable standard of care. Although this credentialing review is at times shifted to the staffing or third-party group providing services, the facility should ensure mechanisms are in place to individualize the approval process for each practitioner providing telehealth services to patients.

2. International

Patient location is typically *the* primary factor when considering which country's licensing and credentialing schemes apply. That is, if a U.S.-based physician were interfacing with a non-U.S. patient in the non-U.S. jurisdiction, that foreign country would typically require the U.S. physician to have a foreign license if patient interaction is for the purpose of making a diagnosis and planning a course of treatment. However, some jurisdictions have more liberal regulations when it comes to medical licensing.

For instance, some European countries provide that if a foreign doctor holds a valid license and is qualified to practice in his or her home country, that is sufficient. Other countries, Like Canada, base their licensing and qualification standards on the number of telehealth visits per year.[11] Medical institutions may also have to be qualified in a non-U.S. jurisdiction as a "health services establishment" or "medical center" in order for their physicians to offer telemedicine services or for the provider to have diagnostic or treatment privileges for his or her patients.[12] In some cases, the U.S.-based practitioner is only consulting with a foreign practitioner, and it is the foreign practitioner that is solely responsible for making diagnosis decisions and implementing treatment plans. Of course, this raises compensation issues for the services provided by U.S. practitioners and potential liability concerns when the foreign practitioner does not adhere to a U.S.-based consultation.

---

[10] IMLC Commission, *A Faster Pathway to Physician Licensure*, INTERSTATE MEDICAL LICENSURE COMPACT https://www.imlcc.org/a-faster-pathway-to-physician-licensure/ (last visited, Jan. 24, 2021).
[11] William F. Ferreira and Adilene Rosales, *United States: International Telemedicine: A Global Regulatory Challenge*, MONDAQ (Mar. 16, 2020), https://www.mondaq.com/unitedstates/healthcare/904170/international-telemedicine-a-global-regulatory-challenge.
[12] *Id.*

U.S. entities utilizing foreign "independent contractors" should also me cognizant of foreign employment laws. For example, healthcare systems using foreign recruiter or procurement agents may believe that the standard "independent contractor" language provides adequate protection from foreign taxes or employment laws. However, that is not always the case. As such, if a system decides to terminate a relationship with an agent, they can be liable for severance payments or other taxation that were not anticipated. In addition, the venue and choice of law provisions are just as important in addressing dispute issues.

C. Liability: Physician-Patient Relationship & Standard of Care

In any medical malpractice case, a plaintiff must first establish that a physician owed her a legal duty to act according to certain professional standards. The plaintiff must show that a contractual, physician-patient relationship was formed. Historically, courts have found that physician-patient relationships can be formed even from simple telephone conversations.[13] In 2011, the Supreme Court of Vermont in *White v. Harris* found that a 90-minute video conference consultation between a physician and individual along with a subsequent written consultation assessment and treatment plan was sufficient to create a doctor-patient relationship.[14] It is not the duration of the doctor-patient relationship that creates a duty, but rather the "doctor's responsibility for the services provided."[15]

In Arizona, in a telehealth setting, a physician is statutorily obligated to obtain verbal or written consent from the patient or the patient's surrogate before the provider delivers care, with few exceptions.[16] The mode of communication—whether by telephone, videoconferencing platform, email, or in-person—does not change the analysis. The core question remains, "did the physician agree to undertake the patient's care and did the patient rely on this undertaking?" If the answer to this question is "yes," a physician-patient relationship has been established.

Next, the plaintiff must show that the provider breached the standard of care. The core question in assessing whether a physician breached the standard of care is whether the individual acted like a reasonably prudent provider under the same or similar circumstances.[17] One issue, however, is that providers have not yet faced the same or similar circumstances that this pandemic has created on such a broad scale. Because the pandemic and virus itself is novel in this age of modern medicine, the law surrounding whether a practitioner has met the standard of care in a telehealth context is playing catch-up to a certain degree.

Even before the widespread use of telemedicine, the trend in medical malpractice cases has shifted from the "locality standard" to a "national standard." That is, a physician has a non-delegable duty to treat each patient with the skill and competence comparable to other physicians in the same field throughout the nation, not just the locality.[18] The national standard not only compares the physician's actions to the national community of practitioners in his field, but also

[13] *Bienz v. Central Suffolk Hosp.*, 557 N.Y.S.2d 139 (N.Y.App. Div. 1990) and *Lyons v. Grether*, 239 S.E.2d 103 (Va. 1977)
[14] *White v. Harris*, 36 A.3d 203, 205 (Vt. 2011).
[15] *Id*. at 207.
[16] A.R.S § 36-3602(A) (2020).
[17] *Weaver v. University of Mich. Bd. of Regents*, 506 N.W.2d 264, 266 (Mich. Ct. App. 1993).
[18] *Hall v. Hilbun*, 466 So. 2d 856 (Miss. 1985).

considers what technologies are available to the physician and the conditions of the facility in which he practices. It seems likely that as medical malpractice cases arise during this pandemic, courts will also consider a physician's acts or omissions in against the backdrop of the health emergency in which the physician exercised judgment.

Moving forward, telemedicine may influence the standard of care analysis if telehealth itself becomes part of the standard. That is, failing to have or use telemedicine, which is becoming an industry standard due to the pandemic, could create liability for providers. If a physician fails to use a telehealth platform correctly or misreads patient data, diagnosis, or imaging, that could certainly create liability for the provider. Having proper safeguards in place for internet security, connectivity, and capacity to store patient data will also be important factors to protect healthcare entities from malpractice suits.

II. Security Issues

A. ePHI Vulnerability

Electronically stored patient health information (known as ePHI) is some of the most coveted data sought after by hackers. Patient health information is easier to target with the advent of cloud computing systems and online patient portals. As more patients interface with their healthcare providers via telehealth platforms during the COVID-19 pandemic, concerns have grown over how to address data privacy concerns.

According to the Department of Health and Human Services, "in just the first half of 2020" there was a 50% increase in the number of healthcare-related cyber-security breaches.[19] The "digital footprint and attack surface" has grown significantly, which makes providers and patients vulnerable to data breaches.[20] In addition, "ransom" has become very lucrative for hackers.

For example, in April 2020, a "foreign actor gained access to [Rangely District Hospital]" in Rio Blanco County, Colorado.[21] The ransomware attack targeted "software necessary to access five years of patient records" and the facility can no longer access "records of patients who received home health services between June 2019 and April 9 . . .."[22] The records contained "names, dates of birth, social security numbers, diagnoses and conditions, and health insurance, claims and billing information."[23] The hospital refused to pay the ransom and the identity of the cybercriminals is still unknown.

However, as discussed below regarding supply chain issues, hospitals do not have an

[19] Brian Bobo, *COVID-19 and health care cybersecurity: How to protect practices and patient data*, MEDICAL ECONOMICS (Oct. 21, 2020), https://www.medicaleconomics.com/view/covid-19-and-cybersecurity-protect-practices-and-patient-data.
[20] *Id.*
[21] Kat Jercich, *Ransomware attack leaves 5 years of patient records inaccessible at Colo. Hospital*, HEALTHCARE IT NEWS (June 16, 2020), https://www.healthcareitnews.com/news/ransomware-attack-leaves-5-years-patient-records-inaccessible-co-hospital.
[22] *Id.*
[23] *Id.*

"exemption" from complying with United States laws concerning payments to prohibited individuals, even when considered the victim. Specifically, on October 1, 2020, the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued an advisory to companies that pay a ransom in the wake of a cyberattack.[24] In essence, OFAC reiterated that payments must not violate economic sanctions laws and the best route is to involve law enforcement as quickly as possible.

But, to avoid such risks, healthcare groups and facilities should do regular IT audits to ensure compliance with best practices related to security. Facilities and groups have spent significant resources over the last twenty years to update informational technology applications to provide higher levels of care and ensure all reimbursable costs are captured. However, it is recognized by the number of ransomware attacks against hospitals that similar resources have not necessarily been applied to security. Facilities and groups can look to the U.S. Government requirements for government contractors as one place to understand the "best practices" associated with cybersecurity, namely those issued by the National Institute of Standards and Technology. Basically, NIST provides an applicable "standard of care" that institutions should be adhering in ensuring cybersecurity.

B. COVID-19 Vaccine Theft

Many healthcare systems are using mobile applications or online surveys to determine which health workers should be prioritized for vaccination. In an effort to streamline distribution, however, healthcare supply chains are now facing security issues with hackers and COVID-19 vaccines actually ending up on the black market and the closer the vaccine gets to a patient, "the greater the risk of diversion."[25]

Where COVID-19 vaccines are distributed in hospitals, they are not always stored in the most-secure places because the vaccines need to be placed in extra-cold storage units.[26] Ironically, technology may actually be the solution to many of these security issues. Vaccines are now being placed into vials "specially made by Corning [which are] embedded with identifies under black light to prevent counterfeits," which is likely to be a bigger concern than theft.[27]

Due to the sensitivities associated with the vaccine distribution plan, facilities authorized to provide the vaccine must not only meet the government requirements associated with such facilitation, but they need to ensure extra security precautions are taken to avoid theft, contamination, or other risks. Facilities should consider reviewing Customs Trade Partnership Against Terrorism guidance concerning facility security best practices that have been utilized successfully for cross-border trade supply security and avoiding diversion, counterfeit, and insertion of contraband.

---

[24] DEP'T OF THE TREASURY, ADVISORY ON POTENTIAL SANCTIONS RISK FOR FACILITATING RANSOMWARE PAYMENTS (2020).
[25] Sharon Goldman, *Covid-19 Vaccines, Vulnerable To Theft, Leave Healthcare Supply Chains Scrambling For Security*, FORBES (Jan. 14, 2021), https://www.forbes.com/sites/sharongoldman/2021/01/14/covid-19-vaccine-vulnerable-to-theft-leaves-healthcare-supply-chains-scrambling-for-security/?sh=3d4bca74ebca.
[26] *Id.*
[27] *Id.*

III. Supply Chain

Supply chain is the "entire process of making and selling commercial goods, including every stage from the supply of materials and the manufacture of the goods through to their distribution and sale."[28] The COVID-19 pandemic has revealed numerous issues in the world-wide supply chain, particularly and notoriously in allocating personal protective equipment ("PPE").

One glaring concern for the global supply chain (that was not necessarily brought on by COVID, but certainly has been exacerbated by the pandemic) is the fact that so much of the world's manufacturing comes from China. Because of such international dependence on Chinese manufacturers, global supply chains for virtually all markets, not just healthcare products, were affected during the initial phases of COVID-19 and which led to a significant spike in PPE costs and associated risks with non-compliant PPE.

Despite countries such as the United States deploying PPE from its Strategic National Stockpiles, overly burdened global supply chains have been unable to efficiently allocate resources because these stockpiles were "not designed to handle a pandemic of this scale."[29] As countries have braced for impact of the "second wave" of COVID-19 and mobilize healthcare workers to roll out the vaccine, supply chain inadequacies undercut efforts to vaccinate efficiently. For instance, last month, healthcare providers in hospitals in "Massachusetts, New York, Arizona, California, and elsewhere" have observed that "those with the most exposure to COVID-19 are not always the first to get vaccinated."[30] Similar supply chain issues surrounding vaccine distribution, testing, and PPE are likewise disrupting efficient allocation of needed resources in the U.K. and other European countries.[31]

Whenever there is a supply shortage of essential products, such as PPE, the tendency is to cut corners on compliance to save on unanticipated increased costs and ensure timely delivery. But, there are significant risks that the healthcare industry cannot fully mitigate by utilizing third party procurement agents, cooperatives, or distribution arrangements. As referenced above, the healthcare industry must comply with international trade laws, including the prohibitions of doing business with denied parties or purchasing products from embargoed countries. This is very similar to the "excluded lists" that the healthcare industry is more familiar. In addition, the industries agents must comply with other trade laws related to, among others, anti-corruption, anti-money laundering, and customs regulations. However, the standard healthcare supply or service agreement rarely include such provisions and instead concentrate on the traditional healthcare regulatory issues, such as anti-kickback and stark law compliance. The reality is that international agreements (for services or supplied), should include all of these provisions.

IV. Counterfeiting

[28] Jack Grimshaw, *What is supply chain? A definitive guide*, SUPPLY CHAIN, https://www.supplychaindigital.com/supply-chain-2/what-supply-chain-definitive-guide (last visited, Jan. 24, 2021).
[29] Daniel J. Finkenstadt, et al., *Why the U.S. Still Has a Severe Shortage of Medical Supplies*, HARVARD BUSINESS REVIEW (Sep. 17, 2020), https://hbr.org/2020/09/why-the-u-s-still-has-a-severe-shortage-of-medical-supplies.
[30] Gabrielle Emanuel, *As Hospitals Roll Out COVID-19 Vaccines Health Care Workers Described And Anger*, NPR (Dec. 28, 2020), https://www.npr.org/2020/12/28/950427961/as-hospitals-rollout-covid-19-vaccines-healthcare-workers-describe-chaos-and-ang.
[31] Shaun Griffin, *Covid-19: Supply chain problems could delay NHS tests*, 371 THE BRITISH MED. J. (2020),

Counterfeiting is a significant problem in the international medical community and has grown over the past months due to COVID-19. As referenced, at the beginning of the pandemic, hospitals scrambled to procure PPE. Quickly though, these healthcare systems realized that the "proliferation of counterfeit PPE . . . has created a gray market" where counterfeiters can easily sell their products to hospitals in desperate need of equipment.[32] Since the pandemic has begun, counterfeiters have "update[ed] classic scams, including impersonating health officials to steal personal information, price gouging and fake treatments" and are implementing "newer schemes like embedding malware in tracing apps."[33]

The U.S. Food and Drug Administration (FDA) and U.S. Immigration and Customs Enforcement (ICE) issued warnings to consumers who might unknowingly purchase fraudulent COVID tests, vaccines, and treatments. By May 2020, Operation "Stolen Promise," an initiative launched by the Homeland Security Investigations arm of ICE, produced 11 arrests and 519 seizures of counterfeit medical supplies.[34] By June 1, 2020, Customs and Border Protection agents had seized around 900,000 COVID-19-realted counterfeits.[35]

The FDA voiced concern over the potential for "deceptive and misleading products" causing Americans to "delay or stop appropriate medical treatment."[36] In response to the growing counterfeiting issue, earlier this month, the bipartisan Safeguarding Therapeutics Act was passed and which authorizes the "U.S. Food and Drug Administration to seize counterfeit medical devices and products, including vaccines."[37]

However, "true" counterfeits are not the only problem. A main issue is whether the products actually meet the specifications that are required by the facility, mandated by regulation, or meet the applicable standard of care to provide the required protection. For example, in the rush to obtain *any* PPE, specifications were not properly laid out in procurement orders. Or, PPE that may actually meet the specifications were obtained from manufacturers that were not authorized by the FDA to provide such items. Thus, PPE (and other products) were received that did not meet the requirements. In some cases, the product may not have been inspected to identify whether

---

[32] Jeff Lagasse, *Healthcare industry is grappling with the emergence of counterfeit PPE in the COVID-19 battle*, HEALTHCARE FINANCE (Aug. 13, 2020), https://www.healthcarefinancenews.com/news/healthcare-industry-grappling-emergence-counterfeit-ppe-covid-19-battle.

[33] Aaron Boyd, *CBP Has Seized Nearly 900,00 Counterfeit and Unsafe COVID-19 Supplies*, NEXTGOV (June 5, 2020), https://www.nextgov.com/cio-briefing/2020/06/cbp-has-seized-nearly-900000-counterfeit-and-unsafe-covid-19-supplies/165959/.

[34] Independent, *Coronavirus: "Poorly constructed" counterfeit masks reaching US health workers*, INDEPENDENT (May 13, 2020), https://www.independent.co.uk/news/world/americas/masks-counterfeit-ppe-health-workers-personal-protective-equipment-us-coronavirus-cdc-a9511326.html.

[35] *Supra* note 29.

[36] FDA, Beware of Fraudulent Coronavirus Tests, Vaccines and Treatments, U.S. Food and Drug Administration, https://www.fda.gov/consumers/consumer-updates/beware-fraudulent-coronavirus-tests-vaccines-and-treatments (last visited, Jan. 24, 2021).

[37] Craig Clough, *Trump Signs Bill Allowing FDA Seizure of Counterfeits*, LAW360 (Jan. 6, 2021), https://www.law360.com/internationaltrade/articles/1342346/trump-signs-bill-allowing-fda-seizure-of-counterfeits?nl_pk=20760519-7208-46af-8693-5588a5eea8a4&utm_source=newsletter&utm_medium=email&utm_campaign=internationaltrade&read_more=1&attachments=true.

specifications were met and, thus, were put into the supply chain. In other case where specifications were not met, facilities were required to utilize subpar product for other functions or donate the products.

Healthcare workers not only faced possible infection as a result of fake PPE, but also were met with threats of retaliation and even termination for speaking out about working conditions.[38] For example, in March 2020, Lauri Mazurkiewicz emailed 50 of her co-workers and supervisors at Northwestern Memorial Hospital "alerting them [that] the standard surgical masks that the hospital required them to wear did not provide adequate protection from COVID-19."[39] In her whistle blower complaint,[40] Mazurkiewicz urged that the hospital provide N95 masks. When Northwestern Memorial refused, she "reported to work wearing an N95 mask from her personal supply . . . [and was subsequently] ordered to remove it."[41] The next day, Mazurkiewicz was fired.

Strapped with depleted or non-existing supply, many hospitals made online solicitations for N95 donations. But federal and state regulations for how to spot counterfeit PPE changed so quickly that it was difficult for healthcare entities to keep up. As such, some hospitals, like Lawrence General Hospital in Massachusetts, handed out counterfeit masks to as many as "40 nurses in a COVID-19 unit before someone noticed."[42] Even worse, in some instances, states knew of CDC warnings about counterfeit masks but nonetheless passed the PPE to "thousands of paramedics and firefighters, prison guards and hospital workers."[43]

Healthcare workers who were denied access to PPE or were terminated because they spoke out about working conditions will find precedent for filing *respondeat superior* claims from the Ebola crisis. In 2014, a nurse, Nina Pham, who contracted Ebola "while caring for the first person to be diagnosed with it in the United States sued the parent company of the Dallas hospital where she worked."[44] Pham alleged that the hospital "wholly failed to ensure that appropriate policies, procedures and equipment were in place."[45]

Of course, there are important fact-specific differences between COVID-19 pandemic and Ebola. This health crisis expanded so quickly and ferociously in the United States that it created an "all-hands-on-deck" situation for healthcare systems. Hospitals were initially given a pass for not having appropriate procedures, policies, or equipment in place for the surge of patients they

---

[38] Olivia Carville, et al., *Hospitals Tell Doctors They'll Be Fired If They Speak Out About Lack of Gear*, BLOOMBERG (Mar. 31, 2020, https://www.bloomberg.com/news/articles/2020-03-31/hospitals-tell-doctors-they-ll-be-fired-if-they-talk-to-press.

[39] Darlene Ricker, *As exposed health care workers seek legal remedies, who's liable for lack of personal protective equipment?* ABA JOURNAL (Apr. 2, 2020), https://www.abajournal.com/web/article/as-exposed-health-care-workers-seek-legal-remedies-whos-liable-for-lack-of-personal-protective-equipment.

[40] Sophie Sherry, *Nurse says she was fired by Northwestern Memorial Hospital after warning co-workers face masks being used were not the safest*, THE CHICAGO TRIBUNE (Mar. 25, 2020), https://www.chicagotribune.com/news/breaking/ct-nurse-northwestern-memorial-hospital-coronavirus-20200324-6smjuxbn6fgnxpaiyzzkjymorq-story.html.

[41] *Supra* note 35.

[42] Juliet Linderman and Martha Mendoza, *Counterfeit masks reaching frontline health workers in U.S*, THE ASSOCIATED PRESS (May 12, 2020), https://apnews.com/article/850d9e6834fc71967af6d3dda65ad874.

[43] *Id*.

[44] *Supra* note 35.

[45] *Id*. (internal quotations omitted).

were tasked with caring for. However, hospitals also have a "legal obligation to provide a safe working environment" for their employees.[46]

At the beginning of the pandemic, when the shortage of PPE was most acute, the CDC released preliminary data finding that 55% of healthcare workers who had tested positive for COVID-19 were exposed at work.[47] Because of the number of confounding factors, it is difficult, if not impossible to identify causation between procurement of fake PPE and workers contracting COVID-19.

However, where healthcare systems knowingly procured fake PPE or had access to legitimate N95 masks but refused to distribute them, they may be held liable for failing to adequately protect their workers. Healthcare entities are likely to face liability for terminating whistleblowers who spoke out about lack of access to legitimate PPE. Liability for healthcare entities who were unable to provide PPE to their workers because of supply chain problem will likely remain tenuous, however.

These supply chain issues are not usually the normal concerns of healthcare attorneys or in-house legal staff. However, facilities should consider performing audits or reviews of its procurement practices to ensure that international laws are followed and quality products are obtained for the safety of both patients and practitioners. Procurement purchase orders should be specific about appropriate specifications for products and rarely allow alternative products that "meet" the specifications, but just the manufacturer has not been approved by the FDA. Procurement departments should consider requiring certifications of quality control from third parties to be included in any shipment. Finally, facilities should consider internal inspection practices to review products received actually meet the required specifications.

V. Offshoring Administrative Support

In an effort to lower administrative costs, facilities and medical groups have increasingly utilized third parties to assist with non-patient administrative tasks, such as medical coding and billing. However, in addition to the significant patient privacy and cybersecurity risks addressed above, there are CMS,[48] individual state regulations, contract provisions, and facility policies related to such practices and that are not always fully understood. One of the main issues is whether the offshore services are "indirect," "incidental," and/or considered "overhead." However, these terms are always clearly defined and lead to confusion. Although confusing regulations are usually interpreted against the regulatory agency,[49] this does not usually provide comfort to legal advisors attempting to comply with the law, but also meeting business realities associated with the increased scrutiny surrounding the costs of healthcare. Although many facilities rely on assurances from the third-party administrative services that such offshoring is compliant, there are usually other provisions in the third-party agreement shifting risk to the

[46] *Id*.
[47] Blake Farmer, *At Least 9,000 U.S. Health Care Workers Sickened With COVID-19, CDC Data Shows*, NPR (Apr. 15, 2020), https://www.npr.org/sections/health-shots/2020/04/15/834920016/at-least-9-000-u-s-health-care-workers-sickened-with-covid-19-cdc-data-shows.
[48] 42 C.F.R. § 438.602 (2016).
[49] *Exxon Mobil Corp. v. Mnuchin*, 430 F. Supp. 3d 220, 243 (N.D. Tex. 2019) (reversing an OFAC penalty on due process grounds where the agency failed to give the regulated party fair notice of the applicable standards).

facility or group. As this is will continue to be a growing area of importance for facilities, regulatory and contractual clarification may be necessary.

VI. CONCLUSION

The days when providing healthcare services were locally concentrated are over. The reality is that, along with the rest of the economy, the business of healthcare is global. The shifting of risk to third-parties, intermediaries, or supply chain cooperatives may not be enough to insulate healthcare facilities and practitioners from the unavoidable risks associated with the global supply chain. As such, legal counsel should consider mitigation strategies that meld traditional domestic laws regulating healthcare services with the ever-evolving laws concerning international trade.