**** Pre-Publication Draft****

The Lure of Foreign Shores: Outsourcing of Overseas Health Care Functions

By Daniel F. Shay, Esq.

Alice G. Gosfield and Associates, P.C.
2309 Delancey Place
Philadelphia, PA 19103
(P) 215-735-2384
(F) 215-735-4778
agosfield@gosfield.com
www.gosfield.com

Accepted for publication in the Health Law Handbook, 2021 Edition. Alice G. Gosfield, Editor, © Thomson Reuters. A complete copy of the Health Law Handbook is available from Thomson Reuters by calling 1-800-328-4880 or online at www.legalsolutions.thomsonreuters.com

The Lure of Foreign Shores:
Outsourcing of Overseas Health Care Functions

By Daniel F. Shay, Esq.

1. Introduction

America currently faces a physician shortage crisis. By 2033, it is currently estimated that there will be a physician shortfall of up to 139,000 physicians.[1] At the same time, technology is rapidly advancing in ways that may be able to help offset the shortage and permit physicians to reach a wider number of patients. In 2015, a remote surgery experiment was performed over a distance of 1200 miles.[2] The experiment simulated a surgery performed by the Florida Hospital Nicholson Center, over the internet, to Ft. Worth, Texas, with a goal of testing the "lag time" (the delay between inputs from the surgeon in Florida, and movements by the simulated robot physically moving the laparoscopic instruments in Ft. Worth). The experiment used a simulator to mimic movements that would be performed by an actual robotic surgical system.[3] No live patients were involved in the surgery, but the experiment demonstrated that remote surgery performed over the internet could be viable.[4]

---

[1] Boyle, Patrick, "U.S. physician shortage growing," Association of American Medical Colleges, June 26, 2020, available at https://www.aamc.org/news-insights/us-physician-shortage-growing.

[2] Mearian, Lucas, "Hospital tests lag time for robotic surgery 1,200 miles away from doctor," Computerworld, May 29, 2015, available at, https://www.computerworld.com/article/2927471/robot-performs-test-surgery-1200-miles-away-from-doctor.html.

[3] The simulation tested lag times that would result from delays in internet service provider processing times. Delays of 200 milliseconds were not noticed by the surgeons. Delays of between 300-500 milliseconds were noticed, but could be compensated for by surgeons pausing their movements. Delays at 600 milliseconds or above, however, led to surgeons becoming insecure about whether they could perform the procedure.

[4] In addition to testing lag times, the experiment also examined the potential impact of a major news event creating bandwidth usage spikes that could delay transmission of data. The Florida hospital successfully accounted for this by using backup connections, further demonstrating that such procedures can be performed even under conditions where bandwidth is suddenly reduced, if appropriate contingencies are in place.

Meanwhile, faced with rising labor costs, the health care industry has taken to outsourcing a range of services overseas, including imaging and other diagnostic testing, transcription, billing and coding, and management services. The drive towards outsourcing is driven by the belief that doing so can reduce financial burdens, especially when outsourcing to countries with dramatically lower overhead and where there is a surplus of highly educated individuals, such as India.[5]

The practice of outsourcing raises a range of issues, however, for health care entities, including compliance with the Health Insurance Portability and Accountability Act of 1996[6] ("HIPAA"), state licensure laws, and contractual concerns. Nevertheless, outsourcing is unlikely to disappear in the face of increasing globalization, and as technology permitting telemedicine itself advances alongside an ever-increasing demand for such services. Although federal health care programs prohibit most payment for clinical services where all or part of the service is rendered overseas, and impose limitations on the degree and nature of administrative tasks which may be performed overseas, health care providers will likely continue to be drawn to outsourcing if it means reducing their bottom line. Towards that end, this article will explore several of the legal issues with which health care providers will have to grapple if they intend to outsource aspects of their business overseas.

2. Offshoring Generally

[5] As a point of clarification, this article will not address in any significant depth the concept of "medical tourism," which is distinct from the type of outsourcing discussed herein. In the "medical tourism" scenario, it is effectively the patients who "outsource" themselves to seek medical treatment overseas, usually where such treatment itself is less expensive and/or when treatment would be considered experimental within the United States. To the extent that the topic is addressed, it is merely to illustrate how it is distinct from the outsourcing of services.

[6] P.L. 104-191.

Within the federal health care context, the offshoring of clinical services is effectively prohibited. Under the Social Security Act and Medicare's billing rules, payment for non-emergency services rendered outside the United States is prohibited.[7] These statutory and regulatory provisions prohibit virtually all overseas clinical services.[8] The prohibition impacts a vast swath of arrangements, including remote diagnostic testing services, remote office visits, and remote surgical services as those become more technologically feasible.

2.1 What Is Not Covered?

Under normal circumstances, Medicare pays for diagnostic testing and certain therapeutic services as long as Medicare's supervision rules and state licensure laws are satisfied.[9] This includes services where part of the service is performed remotely. Thus, diagnostic testing, telehealth services, and chronic care management services are all normally reimbursable when rendered remotely, if applicable requirements are met. However, when the remote party is located overseas, this is not the case; the service will not be reimbursed. Even if the remote physician is, in fact, licensed within the United States, being physically located outside the U.S. renders the service excluded. Moreover, although the COVID-19 pandemic has led Medicare to liberalize much of its attitude towards telehealth services, those liberalizations have not extended

[7] 42 USCA § 1395y(a)(4); 42 CFR § 411.9.

[8] Specifically, the regulation prohibits payment for any services performed outside of the fifty states, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and for shipboard services, the territorial waters adjoining the land areas of the United States. 42 CFR § 411.9(a)(1). There is also an exception for certain emergency services. 42 CFR § 411.9(b).

[9] For more on the contours of diagnostic testing rules under Medicare, see Shay, "Navigating Spaghetti Junction: The Intersection of Medicare's Diagnostic Testing Rules," HEALTH LAW HANDBOOK, 2020 ed., pp. 269-307.

to the prohibition on overseas services.[10] Unless and until Congress passes a law that alters the prohibitions in the Social Security Act, these services will not be reimbursed by Medicare.

2.2 "Nighthawk"/Teleradiology Services

"Nighthawk" services are teleradiology services offered from overseas. This practice usually involves physicians who are trained and licensed in the United States, but who are physically located in time-zones up to eight hours ahead or behind the United States. The distant physicians are used primarily to provide coverage for hospital services. The "Nighthawk" term itself derives from one of the first and most successful companies to implement this business model. Another model, sometimes referred to as the "Indian" model (for the country that is most commonly home to the physicians providing services under the model) involves physicians who are not licensed in the United States, and are therefore less expensive to hire.

In both models, the overseas physician performs a "preliminary" read of a radiology study, usually overnight. The preliminary report is then reviewed, and the service is read again by a physician within the United States, often the following morning. The remotely-located physician's read is then usually described as an "overread." This approach – where the remote physician performs a full interpretation, followed by a local physician's interpretation – is done to meet reimbursement requirements. For example, under Medicare, the U.S.-based physician is required to read the study because, as noted above, Medicare will not pay for services rendered overseas. For the service to be reimbursable, therefore, the local physician must perform the interpretation themselves. The preliminary read, in such circumstances, merely provides the local physician with a starting point for their interpretation.

[10] "COVID-19 Frequently Asked Questions (FAQs) on Medicare Fee-For-Service (FFS) Billings," CMS publication, available at, https://www.cms.gov/files/document/03092020-covid-19-faqs-508.pdf.

It is worth noting that the technical component of such services is still performed in the United States. However, from a technological standpoint, this need not be the case. Depending on the technology used, many services are capable of being performed remotely with the patient only interacting in-person with a medical assistant. Consider the example of remote cardiac monitoring, where the patient is "fitted" with the monitor by a medical assistant, and is then sent home. The monitor device records cardiac events and transmits the recorded data to a remotely-located site where technicians parse the data so that it can be read later by a physician. In such circumstances, the physical location of the technicians is immaterial to the actual performance of the service. For purposes of performing the service, it does not matter if the technicians are located in Milwaukee, Myanmar, or the moon; as long as the data transmission is reliable and the technicians are themselves capable, their physical location – in terms of whether they can perform the service – is irrelevant to their ability to render the service (of course, this does not speak to whether the service will be reimbursable).

There are also "Dayhawk" services, which involve the interpretation of radiology services provided remotely. These services, however, are usually performed by U.S.-based physicians (albeit in remote locations from the patient), operating within the United States, and thereby permitting the billing of their services without the requirement for an "overread" or treating the remote services as "preliminary."

2.3 Offshore Administrative Services

In addition to overseas clinical services like those described above, health care providers may seek to relocate administrative services overseas. These tend to be grouped into two major categories: (1) billing and coding services, and (2) transcription services, although a third category may include the overseas storage of data within electronic health records (EHRs).

Overseas billing and coding services typically submit invoices to patients, manage payments from patients, and submit claims to insurance companies and secondary insurances on the health care providers' behalf. Other services include management of accounts receivable and collections. Offshore billers and coders advertise the quality of the talent that they offer, and flexibility in payment options (e.g., percentage-based payments, per-transaction payments, etc.). They also often promote the nature of the technology they use to perform their services. This makes sense, since such technology is usually a necessity for fast transfer of information between two different countries (indeed, often two different continents). In some instances, they offer practice management software integration with an existing EHR software suite, sometimes with patient portals and patient/customer support as well.[11] Advertising for offshore billing and coding services also may reference buzzwords such as claims to use a "six sigma methodology." For coding services specifically, offshore services may advertise that their coders have the same set of skills as those trained in the United States, but at a lower cost, and cite the benefit of health care providers not having to train or re-train their own employees to perform these tasks.

Interestingly, at least one company within the United States that offered outsourced billing and coding services included on its website testimonials from clients who claimed to have tried overseas billing and coding, and found it unsatisfying. The reasons for the customers' dissatisfaction with overseas services offer insight into areas health care providers would do well to keep in mind when deciding whether to outsource their administrative functions to another country.

[11] For more on issues pertaining to electronic health records software and patient portals, see, Shay, "Physicians Switching EHRs," HEALTH LAW HANDBOOK, 2018 ed., pp. 177-214; Shay, "A Window Into Patient Portals," HEALTH LAW HANDBOOK, 2017 ed., pp. 517-551; Shay, "Downstreamed Physician EHR License Agreements: Understanding the Ebb and Flow," HEALTH LAW HANDBOOK, 2008 ed., pp. 45-76; Shay, "A Primer on Electronic Health Records License Agreements," HEALTH LAW HANDBOOK, 2006 ed., pp. 425-457.

For example, due to time zone differences, to ensure that billing and coding staff were available during hours when the client's business was open, the overseas service had to use "graveyard shift" workers, which increased the risk of errors in coding. In addition, a client testimonial reported that the overseas billers experienced difficulty in navigating state laws and regulatory requirements for filing and coding, and they often lacked familiarity with potential problem areas such as utilization review and medical necessity. This was especially true with respect to state workers' compensation and motor vehicle accident cases, where such issues are governed by state law and regulation. As a result, the client offering the testimonial opted to switch to an outside billing and coding service that was still remote, but based in the United States.

With respect to transcription services, overseas providers often advertise the advanced technology they use. They claim to hire experienced industry professionals, sometimes noting that the level of experience is more than what can normally be found in a traditional hospital transcription environment. These services are also claimed to cost less than comparable U.S.-based transcription.[12] For example, one company noted that the average United States-based transcriptionist is paid between $14 and $15 an hour, whereas an overseas transcriptionist is paid $1 per hour. The companies are also often based in countries where English is spoken widely, such as India or the Philippines. One Philippines-based company advertised that its service complied with HIPAA, and noted that it hired trained and certified medical transcriptionists. Of course, many of the issues that present themselves with respect to overseas billing and coding services are still present for transcription services. Transcriptionists need to be not merely familiar with English, but comfortable with English medical terms and phrases. The "graveyard

[12] This claim could arguably be disputed due to potential decreases in the efficiency of the transcription service.

shift" issues are likewise still present for transcription, and may even be more pronounced, depending on turnaround requirements.

Although not always the case, cloud-based EHRs may also store data overseas on servers located in other countries. This information is not usually referenced in the EHR license agreement, though, and likely is not advertised to health care providers when they are considering whether to purchase a given product. Still, the EHR company itself may opt to use cloud storage which includes overseas cloud storage, again for potential savings.

The major driver spurring health care providers to seek overseas options for their administrative tasks is cost. As noted above, if the health care provider could save $13-14 per hour, per transcriptionist, those costs could be considerable. As margins grow tighter for U.S.-based health care providers, the attraction of low-cost foreign administrative services may be strong. Nevertheless, when considering such an option, there are a range of legal concerns that such providers should bear in mind.

3. HIPAA and Other Security Considerations

Compliance with HIPAA is a persistent concern for U.S.-based health care practitioners. This fact does not change when transmitting protected health information (PHI) to an overseas services provider. The term "PHI" is defined as "Any information that is transmitted or maintained by electronic media or in any other medium, which is individually identifiable."[13] Examples of the type of information that can be considered PHI include names, birth dates, medical record numbers, social security numbers, and other elements.[14] Any entity engaging an

[13] 45 CFR § 160.103.

[14] When data that would be considered PHI are stripped out of a record, the information is considered "de-identified information." For a more complete list of these elements, see 45 CFR § 164.514(b)(2)(i).

overseas service provider that receives PHI from U.S.-based covered entities will be considered a "business associate" under HIPAA, specifically because such entity will not meet the HIPAA definition of "workforce."[15] Because the entity is located offshore, most communications will be electronic – and thus will likely include electronic PHI ("ePHI"), which in turn subjects both the covered entity and overseas the business associate to the HIPAA Security Rule.[16]

The Department of Health and Human Services' Office for Civil Rights (OCR), the government entity tasked with enforcing HIPAA, does not treat overseas services differently under the law than services rendered in the United States. At a baseline, the OCR already generally permits arrangements involving the online transmission of ePHI, including through cloud service providers (CSPs). The OCR has stated that there is no restriction under HIPAA on overseas CSPs handling ePHI.[17] However, although the OCR does not prohibit such practices, it also cautions about the risks involved in such arrangements, and advises that they be considered for the purpose of both the covered entity's and the business associate's risk analyses as required under the HIPAA Security Rule.[18] Specifically, the OCR states, "For example, if ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks, such risks should be considered, and entities must implement reasonable and appropriate technical safeguards to address such threats."[19]

---

[15] Both definitions can be found at 45 CFR § 160.103.

[16] See generally, 45 CFR 164 subpart C.

[17] See, OCR Frequently Asked Question 2083 – "Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside the United States?" Available at, https://www.hhs.gov/hipaa/for-professionals/faq/2083/do-the-hipaa-rules-allow-a-covered-entity-or-business-associate-to-use-a-csp-that-stores-ephi-on-servers-outside-of-the-united-states/index.html.

[18] 45 CFR § 164.308(a)(1)(ii)(A).

[19] OCR Frequently Asked Question 2083 – "Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside the United States?" Available at, https://www.hhs.gov/hipaa/for-

The risks involved in the overseas outsourcing of functions that involve PHI should not be taken lightly by health care providers that qualify as covered entities under HIPAA.[20] The purpose of conducting a security risk assessment is to determine the level of risk posed to the security and integrity of a covered entity's PHI, and to then to justify the steps taken (and not taken) under the circumstances, and demonstrate that the steps taken mitigated such risks. Therefore, in conducting a security risk assessment, the covered entity must be prepared to show that it has considered the risks involved in using an overseas contractor, and believes that those risks either (1) do not present a significant threat, (2) are not likely to occur, and/or (3) can and will be mitigated somehow. If a covered entity uses an overseas services provider located in a country or region with known lax security or increased instances of hacking attempts or other security issues, this could raise the question of why that covered entity used that specific business associate when more secure and/or local options were available. Lower costs, faster turnaround, or other efficiency considerations likely will not be enough to justify the heightened risks involved.[21]

There is, however, some question regarding just how far the OCR's statutory authority actually extends, both from a legal perspective and from a practical one. The HIPAA regulations, including the Omnibus Rule,[22] are clear regarding the OCR's *domestic* authority, but are unclear as to what authority the OCR has to pursue suits against overseas business associates.

---

professionals/faq/2083/do-the-hipaa-rules-allow-a-covered-entity-or-business-associate-to-use-a-csp-that-stores-ephi-on-servers-outside-of-the-united-states/index.html.

[20] For the definition of "covered entity," see 45 CFR § 160.103.

[21] For more on security risk analyses and their role in HIPAA compliance, see Shay, "HIPAA and Meaningful Use Audits and the Security Risk Analysis Nexus," HEALTH LAW HANDBOOK, 2015 ed., pp. 429-464.

[22] 75 Fed. Reg. 5566 (January 25, 2013).

Thus, it is uncertain whether the OCR can impose sanctions on a foreign business for violations of HIPAA as a matter of law. As a practical matter, even if the OCR does have such authority under the law, actively pursuing sanctions against a foreign company on foreign shores would be (a) time consuming, and (b) possibly a waste of resources, especially if the government where the entity is located does not care to involve itself in U.S. enforcement efforts (or worse, is hostile to the U.S. government). As a result, it may make more sense for the OCR to pursue U.S.-based assets of the foreign company, if the company has any. At the same time, the OCR would likely pursue the covered entity, since a failure by the business associate would at least raise the question of whether the covered entity had done sufficient due diligence as part of its own risk analysis.

3.1 Medicare Advantage and Part-D HIPAA Requirements

Medicare Advantage and Medicare Part-D plans also have faced issues relating to HIPAA and its intersection with overseas services providers. In 2006, the Government Accounting Office ("GAO") conducted a study that examined the degree to which Medicare, Medicaid, and TRICARE entities outsourced personal information (e.g., PHI), both domestically and overseas.[23] The report found that, while most Medicare and Medicaid entities did not share personal information overseas with contractors and vendors, (1) some entities were aware that their *contractors and vendors* did share such information overseas with subcontractors, and (2) other entities were *unsure* of whether their contractors or vendors shared such information overseas with subcontractors.[24]

[23] See, GAO-06-676.

[24] GAO-06-676, p.8.

This report, in turn, prompted the publication of a series of memoranda by CMS that would require Medicare Advantage organizations ("MAOs") and Part-D prescription drug plan ("PDP") sponsors to address activities performed outside of the United States.[25] The memoranda required, generally, that offshore subcontractors provide an attestation stating the subcontractor's name and function; the type of PHI provided to the subcontractor; the safeguards adopted to protect beneficiary information; and that the subcontractor conducts an annual audit. This information would also have to be updated within thirty days of any change to it. These obligations continue to the present. In a 2020 publication, the Centers for Medicare and Medicaid Services ("CMS") instructed organizations with offshore subcontractor arrangements to ensure that their data for these subcontractors was up-to-date in accordance with the three memoranda.[26] As a result, MAOs and Part-D PDPs may require in their contracts that their contractors make their own attestations regarding offshore activities, including that such contractors conduct annual audits and report changes within thirty days regarding any such overseas activities. This requires the contractors to pass these obligations on to subcontractors, or imposing restrictions on the parties with which those subcontractors may themselves further subcontract.[27]

3.2 Medicaid HIPAA Concerns

[25] Sponsor Activities Performed Outside of the United States (Offshore Subcontracting), July 23, 2007; Sponsor Activities Performed Outside of the United States (Offshore Subcontracting) Questions & Answers, September 20, 2007; and, Offshore Subcontractor Data Module in HPMS, August 26, 2008.

[26] 2021 Readiness Checklist for Medicare Advantage Organizations, Prescription Drug Plans, Medicare-Medicaid Plans, and Cost Plans, October 2, 2021, p.16.

[27] It is noteworthy, however, that Medicare does not actually prohibit the use of such subcontractors, and merely requests that data be reported.

Similarly, state Medicaid agencies may also place limitations on offshore subcontractor arrangements. In 2014, the Office of Inspector General for the Department of Health and Human Services ("OIG") conducted a review of state Medicaid programs and their requirements regarding offshore outsourcing of administrative functions.[28] The types of administrative functions examined by the report included: enrolling eligible individuals; determining what benefits the Medicaid agency would cover; determining how much the Medicaid agency would pay for covered benefits and from whom it would purchase services; having a system to process claims from fee-for-service providers and making capitation payments to managed care plans; and, ensuring that state and federal health care funds were not spent improperly or fraudulently.[29]

The study examined fifty-six Medicaid agencies, including those of U.S. territories and the District of Columbia, to determine what policies, state laws, contractual requirements, or Executive Orders – if any – the state agencies had in place governing the outsourcing of offshore administrative functions, and whether the agencies did, in fact, engage in such offshore outsourcing. If the agency did have in place outsourcing requirements, the study asked whether the requirements addressed PHI and whether the agency actively monitored contractor compliance with those requirements. In addition, the study looked at agencies' contractual requirements and business associate agreements. For agencies that did engage in offshore outsourcing, the study asked about the types of administrative functions that were outsourced overseas.[30]

---

[28] See, "Offshore Outsourcing of Administrative Functions by State Medicaid Agencies," OEI-09-12-00530, April 11, 2014, available at, https://oig.hhs.gov/oei/reports/oei-09-12-00530.asp.

[29] The full list also includes: monitoring the quality of the services that the Medicaid agency purchased; collecting program information and reporting it to CMS; and, resolving grievances from applicants, beneficiaries, providers, and health plans. OEI-09-12-00530, p. 2.

[30] OEI-09-12-00530, p. 4.

The study determined that only fifteen out of the fifty-six agencies had state-specific requirements addressing outsourcing of administrative functions overseas.[31] The other forty-one agencies had no requirements and did not outsource administrative functions overseas.[32] Of the fifteen agencies that did have rules in place, four agencies prohibited administrative offshore outsourcing, and the remaining eleven permitted the practice.[33] The eleven agencies that permitted such practices did not have in place any additional requirements addressing the safeguarding of PHI.[34] Seven of the eleven reported that they currently outsourced through contractors, and one of the seven actually outsourced directly.[35] The report also noted that offshore outsourcing of administrative functions involving PHI could lead to potential vulnerabilities, due to the limited ability to enforce business associate agreement provisions meant to protect PHI.[36] Specifically, the report stated,

---

[31] OEI-09-12-00530, p.5. For example, Ohio prohibits state executive agencies from entering into contracts that use public funds to purchase services that will be provided outside the United States. Kasich, John R., Executive Order 2011-12K, June 21, 2011, available at https://www.scph.org/sites/default/files/editor/N-002B-EO%202011-12K.pdf. Pennsylvania governor Ed Rendell issued a similar executive order in 2006, which required "All potential contractors who propose to perform contracted services must provide a signed, written certification with their bid or proposal as to those elements or services which will be provided physically or by contract outside of the geographical boundaries of the United States." The order does not prohibit such contracts altogether, but awards points in decisions on proposals to those entities which perform services in the United States. Rendell, Edward G., Executive Order 2006-08, September 14, 2006, available at https://www.oa.pa.gov/Policies/eo/Documents/2006_08.pdf. By contrast, Wisconsin requires its Department of Administration to purchase contractual services "only if those services are performed within the United States," as specified by statute. WSA § 16.705(1r).

[32] OEI-09-12-00530, p.5.

[33] The states permitting the outsourcing of administrative functions offshore to greater or lesser degree are: Florida, Massachusetts, Mississippi, Missouri, Montana, New Jersey, New Mexico, North Dakota, Pennsylvania, Rhode Island, and Tennessee. Tables 1 and 2, OEI-09-12-00530, pp. 7-8.

[34] Tables 1 and 2, OEI-09-12-00530, pp. 7-8.

[35] The states that outsourced through contractors were: Florida, Massachusetts, Mississippi, Montana, North Dakota, and Rhode Island. Missouri engaged in both direct outsourcing and indirect outsourcing through subcontractors. Table 3, OEI-09-12-00530, p. 9.

[36] OEI-09-12-00530, p.7.

> "If Medicaid agencies engage in offshore outsourcing of administrative functions that involve PHI, it could present potential vulnerabilities. For example, Medicaid agencies or domestic contractors who send PHI offshore may have limited means of enforcing provisions of BAAs that are intended to safeguard PHI. Although some countries may have privacy protections greater than those in the United States, other countries may have limited or no privacy protections to support HIPAA compliance."[37]

The risks posed to covered entities by a business associate's failure to adequately secure the covered entity's ePHI – or the failure of an overseas subcontractor – are more than theoretical; they are, in fact, quite real.

3.3 HIPAA Violations and Enforcement

One example of the potential headaches that may be faced by covered entities for the actions of their business associates or subcontractors can be seen in the case of Cogent Healthcare, Inc., which contracted with a business associate – M2ComSys – to perform medical record transcription services overseas in India.[38] The business associate accidentally turned off a firewall used to protect its server that housed otherwise unencrypted PHI, leading to a breach of 32,151 patient records being accessible through basic internet search engines. The firewall was disabled on May 5, 2013, and was not discovered until June 24, 2013. No social security numbers were exposed, but personally identifiable information and medical histories were.[39] The covered entity and business associate were only spared additional enforcement because the activities occurred prior to the September 23, 2013 enforcement date for the HIPAA Omnibus

---

[37] OEI-09-12-00530, p. 7.

[38] In fact, this incident was the second breach of PHI to be suffered by Cogent. McCann, Erin, "Site flaw puts patient data on Google," Healthcare IT News, August 9, 2013, available at https://www.healthcareitnews.com/news/site-flaw-puts-patient-data-google.

[39] "The Wall of Shame: Major Data Breaches of 2013," HIPAA Journal, January 4, 2014, available at, https://www.hipaajournal.com/hipaa-wall-shame-major-data-breaches-2013/.

Rule.[40] Still, they serve as a clear example of how the failures of a business associate could jeopardize the security of a covered entity's PHI.

Another example of overseas business associate actions exposing covered entities to liability can be seen in a lawsuit filed against MDLive, a telehealth company. In April, 2017, MDLive was sued in a class action suit alleging that it had violated HIPAA by sharing PHI with an overseas business associate. As part of its own efforts to test the performance of its telehealth app, MDLive used an app developed by the Israeli company TestFairy. One function of the TestFairy app was to take screenshots of MDLive's app when these screenshots could include patient PHI.[41] Ultimately, the lawsuit was dropped – without a monetary settlement – in June, 2017 when the plaintiff voluntarily dismissed the case.[42] It is likely that the case did not extend much past the initial discovery phase.

MDLive, around this same time, published a public fact sheet that refuted the claims in the lawsuit.[43] In the fact sheet, MDLive stated that there had been no HIPAA violation, that no PHI had been improperly shared, patient data was safe, and TestFairy was contractually required to maintain the privacy and security of PHI provided to it by MDLive. The fact sheet also noted that MDLive's own privacy policies indicated that patient data might be disclosed to third party

[40] Specifically, the OCR stated that it, because the activities occurred before the enforcement date, the OCR "provided the [business associate] with technical assistance regarding current HIPAA Privacy and Security Rule [business associate] requirements." This information is available through the OCR's web portal for data breaches, in the "Archive" section, available at https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[41] Comstock, Jonah, "MDLive faces class action suit over alleged data privacy breach," mobihealthnews.com, April 25, 2017, available at, https://www.mobihealthnews.com/content/mdlive-faces-class-action-suit-over-alleged-data-privacy-breach.

[42] Comstock, Jonah, "Privacy lawsuit against MDLive abruptly dropped," mobihealthnews.com, June 5, 2017, available at, https://www.mobihealthnews.com/content/privacy-lawsuit-against-mdlive-abruptly-dropped.

[43] "MDLive Fact vs. Fiction," available at https://welcome.mdlive.com/wp-content/uploads/2017/04/MDLive-Fiction_vs._Fact-Sheet_ATA-4.23.17.pdf.

entities to support MDLive's own business. All of this suggests that MDLive had a business associate agreement in place with TestFairy, and obligated TestFairy – under the terms of the business associate agreement – to comply with HIPAA's requirements.[44] The screenshots taken by the TestFairy app allegedly contained images that could include patient histories, which in and of themselves may not have violated HIPAA, unless the "minimum necessary" standard was violated.[45] It is also possible that the lawsuit was dropped simply because there is no private right of action under HIPAA. If the suit was filed as a class action under HIPAA itself, then it would not have survived a motion to dismiss, and once this fact was discovered, the plaintiff might have simply dropped the case rather than spend the time and money on discovery.

Nevertheless, while the case did not result in MDLive being required to recompense any damages, it does highlight the type of arrangement that could lead to problems for a covered entity. The case involved an overseas business associate where the activities of the business associate potentially endangered the PHI. MDLive stated that it had contracts in place to protect PHI (likely a business associate agreement). However, a business associate agreement alone would not be enough to protect a covered entity, even in the case of a business associate gone wild. Moreover, although there is no private right of action under HIPAA itself, the covered entity would still face the risk of HIPAA enforcement by the OCR, and could also face civil liability under state confidentiality laws.

---

[44] Business associates also have direct liability under HIPAA. 42 USCA §§ 17931, 17934.

[45] Comstock, Jonah, "MDLive faces class action suit over alleged data privacy breach," mobihealthnews.com, April 25, 2017, available at, https://www.mobihealthnews.com/content/mdlive-faces-class-action-suit-over-alleged-data-privacy-breach. The "minimum necessary" rule under HIPAA, which generally only permits covered entities to disclose the "minimum necessary" amount of PHI to accomplish the task at hand. See, 45 CFR § 164.514(d).

Finally, consider the example of CHSPSC, LLC, a business associate of Community Health Systems, Inc. ("CHS"), which provided a range of administrative, management, and legal services to CHS-owned entities.[46] The case did not involve an overseas subcontractor's breach, but does help illustrate the potential impact of a business associate's data breach on both the business associate and the covered entity. On April 10, 2014, CHSPSC suffered a breach of PHI arising from a hack that involved compromised administrative credentials, allowing hackers to access CHSPSC's information system through the company's virtual private network.[47] The company remained unaware of this breach until the Federal Bureau of Investigation notified it eight days after the cyber-attack began.[48] The hack itself affected two-hundred thirty-seven covered entities served by CHSPSC, and involved the theft of approximately six million individuals' PHI, including data such as names, sex, dates of birth, phone numbers, social security numbers, ethnicities, email addresses, and emergency contact information.[49]

The OCR ultimately determined that CHSPSC had failed to: (1) prevent the attack in the first place; (2) respond to and document a known security incident; (3) mitigate the harmful effects of the hack; (4) implement technical policies and procedures to permit only authorized individuals or software to access its information systems; (5) implement policies and procedures to regularly review records of information systems activity (e.g., audit logs, access reports, etc.); and (6) conduct an effective security risk assessment to determine the risk and vulnerability to

[46] In fact, CHSPSC, LLC was itself owned by CHS, Inc., but operated as a business associate of the CHS entities. See, Resolution Agreement, available at the OCR's website at https://www.hhs.gov/sites/default/files/chspsc-ra-cap.pdf.

[47] Resolution Agreement, Section I.2, p.1.

[48] Resolution Agreement, Section I.2, p.1.

[49] Resolution Agreement, Section I.2, p.1.

the confidentiality, integrity, and availability of the electronic PHI in its possession.[50] As a result, CHSPSC paid $2.3 million for the breach, and entered into a resolution agreement with the OCR, including a corrective action plan.[51] In addition, the CHS parent company itself entered into a settlement with twenty-eight states for this same violation, and for its own failure to implement and maintain appropriate security for the information collected and held by CHS and its business associate subsidiary.[52] This led CHS to pay an additional $5 million in its own settlement, in addition to agreeing to comply with a range of laws (including HIPAA), as well as to develop, implement, and maintain a written information security program designed to protect the security, integrity, and confidentiality of personal information and PHI collected, stored, transmitted, and/or maintained by CHS.[53] In addition, CHS entered into a settlement agreement in response to a class action suit brought by the individuals whose PHI and personal information were part of the breach, agreeing to pay an additional $3.1 million to settle the suit.[54] This brings the total payments made by CHS or CHS-related entities to $10.4 million, which does not

[50] Resolution Agreement, Sections I.2.A-I.2.E, pp.1-2.

[51] Resolution Agreement, Section II.1, p.2.

[52] "Hospital system agrees to pay $5 million over data breach," Press Release, Iowa Attorney General's Office, October 8, 2020, available at https://www.iowaattorneygeneral.gov/newsroom/chs-community-data-breach-settlement.

[53] Consent decree, Section 26, p. 6. This included a list of requirements for the program, such as it: being documented in writing; permitting access to PHI only to the extent necessary for each user to perform job functions or assignments; requiring CHSPSC to employ an executive or officer – with training, expertise, and experience in information security – to a full-time position tasked with implementing, maintaining, and monitoring the program; developing an incident-response plan to address security events; develop a specific patch management policy to address requirements for applying security updates and security patches; and, incorporating security awareness and privacy training for all personnel with access to PHI. Consent decree, Section 26, pp. 6-8.

[54] Ellison, Ayla, "CHS reaches settlement with 4.5M patients affected by data breach," Becker's Hospital Review, February 5, 2019, available at https://www.beckershospitalreview.com/legal-regulatory-issues/chs-reaches-settlement-with-4-5m-patients-affected-by-data-breach.html. The settlement itself can be accessed at https://chspscsettlement.com/Content/Documents/Settlement%20Agreement.pdf.

begin to take into account whatever expenses the CHS entities undertook to achieve compliance with the various settlements, resolution agreements, and laws, with all of these expenses ultimately arising from the failure of a business associate to effectively manage the PHI provided to it by covered entities.

4. Licensure and State Law Issues

When clinical work is provided by overseas physicians, it necessarily raises the issue of compliance with state licensure and telehealth laws.[55] At a baseline, any overseas physician treating a patient must meet the licensure requirements of the state where the patient is being treated, although these licensure requirements vary from state to state. The COVID-19 pandemic has also resulted in the liberalization of licensure requirements, although these too vary from state to state. Assuming the licensure requirement is met, there may be additional limitations for overseas physicians with respect to the types of services that may be performed by non-physician personnel, and those too may vary under state law, depending on the type of personnel.

4.1 Licensure Requirements

State laws require physicians to be licensed to treat patients located within their states. These requirements, however, vary depending on the state. Many states require that the physician hold a full, unrestricted license within that state to perform services, regardless of whether the physician is physically located in-state or elsewhere.

For example, Delaware law requires that physicians hold a license to practice medicine in state, and does not have a separate category of licensure specifically for telemedicine.[56]

---

[55] For an overview of legal issues pertaining to telehealth, see Kass, Julie and Alison Cohen, "Telehealth and Technology-Based Care: Developments and Implications," HEALTH LAW HANDBOOK, 2021 ed., pp. ***[TBD]***.

[56] 24 Del C. § 1720(a)(1).

Kentucky likewise generally requires a license to practice medicine without regard to the location of the physician, and does not have a separate licensure category for telemedicine providers.[57] Ohio also does not recognize a separate category of licensure for telemedicine, and in fact eliminated their telemedicine certificate (which functioned as a separate licensure category) in 2019.[58] Some states generally require licensure, but permit physicians in adjoining states to practice medicine when treating patients who are located in-state, or to treat patients when the physician already has an established physician-patient relationship with the patient.[59]

Other states, however, recognize broader categories of licensure for telemedicine. Georgia, for example, permits physicians to obtain telemedicine licenses specifically.[60] Minnesota likewise has a licensure category for the interstate practice of telemedicine.[61] New Mexico also recognizes a separate category of licensure for the provision of telemedicine

[57] KRS § 311.560(1).

[58] See, Ohio Rev. Code Ann. § 4731.09 for Ohio's licensure requirements generally. The former provision at Ohio Rev. Code Ann. § 4731.296 was repealed in 2019 with the passage of 2019 Ohio Laws File 10 (Am. Sub. H.B. 166).

[59] For example, Arizona permits physicians licensed to practice in another jurisdiction to treat patients when the patient resides outside of Arizona and both the physician and patient are located in-state for a period of not more than sixty consecutive days. A.R.S. § 32-1421(B)(2). Maryland permits physicians located in adjoining states to prescribe home health services to patients residing in Maryland if the physician does not have an in-state office, and the physician has performed an in-person physical examination of the patient within the adjoining state where the physician is located. MD Code, Health Occ. § 14-302(4). Connecticut likewise permits physicians residing out of state who are employed to come into Connecticut to treat patients located in-state for a limited period of thirty days. C.G.S.A. § 20-9(b)(5). Ohio permits physicians located on the border of a contiguous state, whose practice extends within Ohio to treat patients as long as the physician does not in person or through the use of any communications (including electronic communications) open an office to see patient or receive calls from within Ohio. Ohio Rev. Code Ann. § 4731.36(A)(5).

[60] O.C.G.A. § 43-34-31.1.

[61] M.S.A. § 147.032. The precise wording of this provision, however, could raise questions about its application to *overseas* licensees. Specifically, the criteria for a telemedicine license includes that "the physician is licensed without restriction to practice medicine in the *state* from which the physician provides telemedicine services." M.S.A. § 147.032(a)(1). However, another requirement is that "the physician has not had a license to practice medicine revoked or restricted in any state *or jurisdiction*," thereby apparently recognizing the distinction between a "state" and a "jurisdiction." The statute does not provide a definition for either term, however.

services, but interestingly this requirement only applies to physicians licensed to practice in another state or territory of the United States; this would preclude the practice of medicine using telemedicine technology from overseas, unless the physician has a license in another state already (in effect, resulting in the physician "daisy-chaining" their way into a New Mexico telemedicine license).[62]

Many states do not require in-state licensure for an otherwise licensed physician to provide periodic consultations in-state.[63] Such laws can serve to permit the operation of "Nighthawk" and "Dayhawk" style services, where the out-of-state physician's interpretation is merely a preliminary read, and an in-state physician follows up to perform the interpretation upon which patient care decisions are made. However, at least one state, Connecticut, explicitly requires full licensure for any physician "whose practice of medicine include any ongoing, regular or contractual arrangement" where the physician provides "through electronic communications or interstate commerce, diagnostic or treatment services, including primary diagnosis of pathology specimens, slides or images," and which states that with respect to radiographic images, "licensure shall be required for an out-of-state physician who provides, through an ongoing, regular or contractual arrangement, official written reports of diagnostic evaluations of such images to physicians or patients in this state."[64]

For example, the state of New Jersey expedited the processing of out-of-state licensure for physicians, and has waived the requirement to obtain licensure when the physician is not

[62] N.M.S.A. 1978 § 61-6-11.1.

[63] See, Ohio Rev. Stat. Ann. § 4371.36(A)(3); K.R.S. § 311.560(2)(b); 24 Del. C. § 1727; C.G.S.A. § 20-9(a)(4); A.R.S. § 32.1421(B)(1); MD Code, Health Occ. § 14-302(2)(i).

[64] C.G.S.A. § 20-9(d).

license in-state, but has an established relationship with the patient in question, and those who have no such relationship may provide services to patients in New Jersey as long as they only provide screening, testing, and treatment for COVID-19.[65] On March 20, 2020, Governor Brian Kemp of Georgia issued an executive order which, among other things, instructed the Georgia Composite Medical Board to immediately adopt emergency rules to provide telemedicine licenses in accordance with state law.[66] Also in response to the COVID-19 emergency, the Board generally began to expedite licensure applications.[67] On March 18, 2020, Governor Tom Wolf of Pennsylvania similarly issued an executive order which, among other things, temporarily suspended the requirement for out-of-state practitioners to be licensed in Pennsylvania to practice telemedicine, as long as they were licensed in good standing in their home state, territory or country by the equivalent professional board.[68] Other states have similarly relaxed their requirements. It remains to be seen how many of these changes survive the COVID-19 emergency, although it seems reasonable to expect that states will once again at least require that out-of-state physicians obtain some form of licensure in those states where licensure requirements were eliminated or relaxed. However, in the wake of the crisis, states may further liberalize and modernize their telemedicine licensure laws (or, indeed, adopt them at all if they do not currently have any). Nevertheless, any business attempting to utilize the clinical services

[65] See, "Telehealth Services During the COVID-19 Pandemic Frequently Asked Questions (FAQs)," revised October 30, 2020, available at https://www.njconsumeraffairs.gov/COVID19/Documents/FAQ-Telehealth.pdf.

[66] Executive Order, "Reducing Regulations to Assist the State's Response to the Spread of COVID-19," available at, https://gov.georgia.gov/executive-action/executive-orders/2020-executive-orders.

[67] See, GCMB Emergency Practice Permit/Temp License in response to COVID-19, available at https://medicalboard.georgia.gov/press-releases/2020-03-16/gcmb-emergency-practice-permittemp-license-response-covid-19.

[68] See, Executive Order, "Order of the Governor of the Commonwealth of Pennsylvania to Enhance Protections for Health Care Professionals," available at https://www.governor.pa.gov/wp-content/uploads/2020/05/20200506-GOV-health-care-professionals-protection-order-COVID-19.pdf.

of a physician located overseas will need to carefully navigate the state law licensure requirements.

4.2 Supervision of Non-Physician Personnel

Regardless of the hurdles that overseas health care practitioners must surmount to obtain licensure to render telehealth or telemedicine services, once they have an appropriate license, they must be able to supervise other personnel. Modern medical practice relies heavily upon the use of a broad range of personnel to assist in the delivery of clinical services. Medical assistants, radiology technicians, and a variety of so-called "mid-level" or "advanced practice" health care practitioners (such as physician assistants and nurse practitioners) are essential to the actual delivery of health care.[69] However, state law usually requires physician involvement with the activities of these practitioners, to a greater or lesser degree. This necessarily raises the question of what types of services these individuals may perform without the physical presence of a physician. In other words, what impact does a physician being overseas have on the scope of services that may be provided by the physician's subordinates and allied health professionals?

This answer, too, depends greatly on state law. In many cases, state law permits physicians to provide remote, electronic supervision rather than requiring their physical presence. This is especially true with respect to physician assistants and nurse practitioners in their licensure laws and regulations. For example, Pennsylvania law requires only that a physician providing supervision to a physician assistant or nurse practitioner be available via telephone, radio, or telecommunications to provide supervision or collaborative support.[70]

---

[69] For a more in-depth discussion of these types of practitioners, their role in health care, and the legal issues that face them, see, Shay, Daniel, "Highest and Best Use Revisited," HEALTH LAW HANDBOOK, 2013 ed., pp. 309-344.

[70] For physician assistants, Pennsylvania law defines "supervision" to mean "Oversight and personal direction of, and responsibility for, the medical services rendered by a physician assistant. *The constant physical presence of the*

Similarly, New Jersey permits physician assistants to be supervised by a physician using electronic supervision.[71] Florida defines "supervision" for PAs as meaning that the physician is "easily available," such as via telecommunication.[72] California likewise permits physicians to provide supervision to physician assistants by remaining available by telephone or electronic communication when the physician assistant is examining a patient.[73] In Illinois, "physician assistant practice" requires collaboration with a physician, but collaboration is not meant "to necessarily require the personal presence of the collaborating physician at all times at the place where services are rendered, as long as there is communication available for consultation by radio, telephone, telecommunications, or electronic communications."[74] Collaborative agreements must also set forth which procedures require the physical presence of the collaborating physician.[75] Georgia state law generally does not require the physical presence of

---

supervising physician is not required so long as the supervising physician and the physician assistant are, or can be, easily in contact with each other by radio, telephone or other telecommunications device." 49 Pa. Code § 18.122, emphasis added. For nurse practitioners, "collaboration" is defined to include "Immediate availability of a licensed physician to a [certified registered nurse practitioner] through direct communications *or by radio, telephone or telecommunications.*" 49 Pa. Code § 21.251, emphasis added.

[71] NJAC § 13:35-2B.10(b). New Jersey law states, "Supervision of a physician assistant shall be continuous but shall not be construed as necessarily requiring the physical presence of the supervising physician, provided that the supervising physician and physician assistant maintain contact through electronic or other means of communication."

[72] FSA § 458.347(2)(f). The definition reads "'Supervision' means responsible supervision and control. Except in cases of emergency, supervision requires the easy availability or physical presence of the licensed physician for consultation and direction of the actions of the physician assistant. *For the purposes of this definition, the term 'easy availability' includes the ability to communicate by way of telecommunications.* The boards shall establish rules as to what constitutes responsible supervision of the physician assistant." Emphasis added.

[73] Cal. Bus. & Prof. Code § 3501(f)(1)(B). The law states, "'Supervision' means that a licensed physician and surgeon oversees the activities of, and accepts responsibility for, the medical services rendered by a physician assistant. Supervision, as defined in this subdivision, *shall not be construed to require the physical presence of the physician and surgeon*, but does require the following: …(B) *The physician and surgeon being available by telephone or other electronic communication method at the time the PA examines the patient.*" Emphasis added.

[74] 225 ILCS § 95/4(3.5).

[75] 225 ILCS § 95/7.5(a)(1).

a physician for the physician assistant to perform assigned duties, but permits the physician assistant to perform duties even outside the scope of their job description when the physician is physically present.[76]

Supervision requirements for medical assistants and technicians, by contrast, is a less clear and sometimes more restrictive matter. For example, Florida explicitly requires direct supervision of medical assistants by a physician for the medical assistant to perform most tasks.[77] Florida's regulations define "direct supervision" to require the physical presence of the physician.[78] Montana requires that a physician provide to the medical assistant "onsite direct supervision"[79] for injections (other than immunizations), invasive procedures, conscious sedation monitoring, allergy testing, intravenous administration of blood products, or intravenous

[76] Specifically, Georgia law, in defining the scope of practice for physician assistants, states "Nothing in this article shall prohibit the rendering of services to a patient by a physician assistant who is not in the physical presence of the supervising physician, or preclude…performing any functions authorized by the supervising physician which the physician assistant is qualified to perform." OCGA § 43-34-103(d). Instead, Georgia law states that, "When a patient receives medical services from a physician assistant, the supervising physician's involvement in the patient's care, including patient evaluation and follow-up care by the supervising physician, shall be appropriate to the nature of the practice and the acuity of the patient's medical issue, as determined by the supervising physician." OCGA § 43-34-109. Georgia law also states, "…nothing in this Code section shall make unlawful the performance of a medical task by the physician assistant, whether or not such task is specified in the general job description, when it is performed under the direct supervision and in the presence of the physician utilizing him or her." OCGA § 43-34-105.

[77] FSA § 458.3485(2). Among the duties that require direct supervision are: taking vital signs, preparing patients for the physician's care, observing and reporting patients' signs or symptoms, assisting with patient examinations and treatment, operating office medical equipment, collecting routine laboratory specimens as directed by the physician, and performing office procedures including all general administrative duties required by the physician.

[78] FAC § 64B8-2.001(1)(a). "'Direct supervision' shall require the physical presence of the supervising licensee on the premises so that the supervising licensee is reasonably available as needed." By contrast, "Indirect supervision" is defined to "require only that the supervising licensee practice at a location which is within close physical proximity of the practice location of the supervised licensee and that the supervising licensee must be readily available for consultation as needed. 'Close physical proximity' shall be within 20 miles or 30 minutes unless otherwise authorized by the [Board of Medicine]." FAC § 64B8-2.001(1)(b).

[79] Itself defined to mean, "physically present in the same building; or in sufficiently close proximity to the person under supervision to be quickly available to the person under supervision." ARM § 24.56.601(7).

administration of medication.[80] Georgia does not license medical assistants, but rather recognizes their practice in their medical licensure laws, which permit a physician to delegate certain tasks to a medical assistant, and which requires the physician to be "on-site" for the performance of some of those services, but not for the medical assistant to obtain vital signs.[81] Under California law, medical assistants are permitted to administer medication by intradermal, subcutaneous, or intramuscular injections, perform skin tests, and perform additional technical support services upon the specific authorization and supervision of a licensed physician. However, California defines "supervision" in this context as requiring the physical presence of the supervisor in the treatment facility during the performance of the procedure.[82]

As a practical matter, state law requirements for the physician's physical presence on site to provide supervision necessarily limit the scope of clinical work that can be performed when the physician is off-site, which in turn can implicate the full range of clinical services available under overseas outsourcing arrangements. For example, it is difficult to imagine a physician practice operating with a physician physically located in another country, when the practice requires the use of medical assistants to, for example, take patient vital signs, if state law requires the physical presence of the physician to provide supervision to the medical assistants.

By contrast, "Nighthawk" models involving remote diagnostic services which can function with a physically distant physician to perform interpretation of clinical information can

[80] ARM 24.156.401(3)(c).

[81] Specifically, Georgia permits physicians to delegate to a medical assistant: subcutaneous and intramuscular injections; obtaining vital signs; administering nebulizer treatments; or removing sutures and changing dressings. Ga. Comp. R. & Regs. §360-3-.05(1)(a)(1)(i). However, the physician must be on-site for the administration of subcutaneous and intramuscular objections, nebulizer treatments, and the removal of sutures and changing of dressings. Ga. Comp. R. & Regs. §360-3-.05(1)(a)(1)(ii).

[82] Cal Bus. & Prof. Code § 2069(a)(1), (b)(3).

be made to work even if state law requires a physician's physical presence. In such an arrangement, the remote physician is only being used for their specialized knowledge and to perform the specific task of providing interpretation of collected information, while an on-site physician may be present to provide the necessary supervision to allow medical assistants or technicians to collect relevant data.

5. Malpractice Concerns

While HIPAA compliance and state licensure law compliance are the most obvious and immediate concerns for U.S.-based entities considering overseas outsourcing, overseas outsourcing of clinical functions also brings with it the potential for malpractice exposure, with "Nighthawk"-style arrangements implicating both the monitoring company providing the Nighthawk services themselves, and the entity with which they've contracted. In other words, as a result of the actions of a downstreamed overseas clinical services entity, the upstream contracting entity may be forced to defend itself in a malpractice suit.

Consider, for example, the case of Young v. Naples Community Hospital.[83] In the case, a patient presented at the emergency room complaining of abdominal pain and vomiting. In response, the emergency physician on call ordered a CT scan of the patient. The scan was performed and read preliminarily by a physician located in Switzerland who had entered into an independent contractor relationship with Nighthawk Radiology Services, LLC. The physician reported seeing "unremarkable" results. The patient was admitted nonetheless, and later had a magnetic resonance angiogram performed, which revealed other complications. The original CT scan image was then later reviewed "by other personnel," and it was found to show a potential

[83] 2014 WL 26040, 129 So.3d 456 (Fl. App. 2014).

blood clot, which required surgical intervention to remove.[84] The patient sued the hospital, the U.S. radiology group, Nighthawk Radiology, and the overseas physician in malpractice, with the patient winning after a jury trial.[85]

Florida law required that defendants in the case be provided with notice the plaintiff's intent to sue within two years of the injury, which the hospital was given. However, the notice was not provided to either Nighthawk or the remote radiologist.[86] The case turned on the question of whether Nighthawk and its physician had been properly notified. The Nighthawk defendant argued that the statute of limitations had run, due to the plaintiff's failure to provide timely notice of the plaintiff's intent to sue, as required under Florida law. A Florida appellate court held that the notice requirement of the law was satisfied and that notice had been properly given due to the contractual relationship between the U.S. radiology group and Nighthawk (and by extension, between Nighthawk and its independent contractor physician).[87] In other words, because of the chain of contracts, notice provided to the U.S. radiology group was sufficient to notify Nighthawk and the overseas radiologist.

In this case, both downstream and upstream entities were named as defendant, requiring all to undertake the time and expense of the defense itself, even if the upstream parties (e.g., the hospital and emergency physician) had been able to obtain dismissal of claims against them. Moreover, under Florida law, the failure to serve specific notice on one of the sub-contracted parties did not permit the statute of limitations to run out in that sub-contractor's favor. Thus,

---

[84] 129 So.3d. 457.

[85] The facts of the case can be found at 129 So.3d 457-459.

[86] 129 So.3d 458-459.

[87] 129 So.3d 460-461.

the legal action taken against the upstream/hiring entity resulted in liability applying to the downstream entity, even as the actions of the downstream entity potentially created the situation under which the upstream entity was sued in the first place.

Another example from Pennsylvania is that of Palar v. Wohlwend, et al.,[88] wherein a patient presented at the patient's primary care physician complaining of back pain. The physician referred the patient to a hospital for two magnetic resonance imaging (MRI) scans of the spine – one performed in March, 2009, and another in April of the same year. The hospital radiologist obtained the MRI images and sent them to a teleradiology company to review. The teleradiologist reviewed the images and did not note any abnormalities in the lungs. In 2010, the patient developed a cough and was sent to the same hospital for a chest x-ray, which was reviewed by the same radiologist, and who reported no significant pathology. Additional chest x-rays resulting from continued coughing were performed in 2012 and in 2013, this time to determine whether the cause was asthma. Again, these scans were reviewed by the same radiologist. By 2014, the patient was diagnosed with lung cancer, which had metastasized to the brain, and which doctors determined would prove fatal. The plaintiff (the deceased patient's estate) sued the hospital, the radiologist, the teleradiologist, and the teleradiology company, winning a $3 million verdict at trial, with liability apportioned equally between the teleradiology defendants on the one hand, and the hospital and radiologist on the other.[89]

Following the trial, the teleradiology defendants appealed and requested a judgment notwithstanding the verdict. The teleradiologist defendants argued that the hospital's on-site

[88] 2017 WL 243470 (Pa. Super. 2017).

[89] The factual basis of the case can be found at 2017 WL 243470, *1-*2.

radiologist could have discovered the cancer in the interim and thereby minimized the damage.[90] The appellate court examined the arguments raised regarding deviation from the standard of care and relative liability, but ultimately determined that there was evidence to support that the teleradiologist had indeed failed to perform to the standard of care, increasing the patient's risk of harm, and noting that the jury had apportioned liability equally, which necessarily meant that the jury had not found sufficient evidence to divest the teleradiologist of liability.[91]

Again, the case offers an example of how teleradiology arrangements can result in each party bearing liability, as well as what happens at trial when the parties attempt to shift liability to each other. In this case, the downstream entity attempted (albeit unsuccessfully) to shift liability to the upstream one. Although the teleradiologist in this case was located within the United States, it is not difficult to envision an overseas clinical provider and/or the company that employs them taking the same approach.

The third example – a recent one – presents a complex fact pattern. In Shicheng Guo v. Kamal,[92] an Illinois patient presented at the emergency room of a hospital complaining of a sudden-onset headache on July 10, 2013. The emergency room physician ordered a CT scan of the patient's head, and a teleradiologist employed with a teleradiology company interpreted the head CT scan, finding no evidence of a brain bleed. Therefore, at 3:20 am, July 11, 2013, the patient was discharged. Later that same morning, the attending radiologist at the hospital performed a secondary read of the CT scan and identified a subarachnoid brain hemorrhage. At 9:00 am, the patient was called to return to the emergency room, and at 10:30 am, another

[90] The procedural history of the case can be found at 2017 WL 243470, *2.

[91] 2017 WL 243470, *5.

[92] 155 N.E.3d. 517 (Ill. App. 2020).

emergency room physician informed the patient of the brain bleed, recommending that the patient be admitted to the hospital for further evaluation or treatment. The patient, however, declined. At 11:00 am on the same day, the patient presented at a the emergency room of a *different* hospital, and was seen by an emergency physician, who ordered another CT scan, which was performed at 11:15 am. The results of this scan were interpreted as normal, and no brain bleed was found. The patient consulted with a neurosurgeon, who learned of the patient's history, including the previous CT scan at the first hospital, and who obtained the radiology *report* from the first hospital.[93] The neurosurgeon ordered a CT angiogram, which also produced an image that was interpreted as normal. Thereafter, the patient was discharged from the second hospital. Four days later, the patient died and a pathologist's report determined that the cause of death was an intracerebral hemorrhage *unrelated* to any of the bleeds found in the previous few days. The patient's family sued the first hospital, the first teleradiologist, the first teleradiology company (under a theory of *respondeat superior*), the second hospital, and others.[94]

The teleradiologist, teleradiology company, and first hospital all moved for summary judgment, arguing that there was insufficient evidence to prove that the brain bleed the teleradiology defendants had failed to identify had proximately caused the patient's death, nor affected the eventual course of care at the second hospital.[95] Overruling the trial court, the appellate court held that there was evidence presented to at least raise a genuine issue of material fact (e.g., whether if the teleradiologist had correctly identified the brain bleed, or the images of the first CT scan had been provided alongside the report, would have led to a different course of

[93] Note: the *images* themselves, however, were neither obtained nor sent. Shicheng Guo, at 521.

[94] The full fact pattern can be found at 155 N.E.3d. 520-521.

[95] The procedural history of the case can be found at 155 N.E.3d. 521-522.

treatment that would have more effectively treated the hypertension that eventually led to the patient's death), and therefore summary judgment must be denied.[96]

Each case described above involved the parties attempting to disclaim their own liability, and in some cases with downstream entities attempting to shift liability to upstream ones. To the extent that it could be proven in any of the cases that the teleradiology parties had caused the various injuries, that still would not have effectively protected the upstream parties from having to defend the cases, even if they were ultimately determined to not bear any liability. By its nature, teleradiology necessarily increases the total number of parties with an impact on the patient's condition simply because it adds to the list of potential defendants the teleradiologist and (when applicable) the teleradiology company that has hired the teleradiologist. Moreover, depending on the laws of the jurisdiction, the degree of liability for the patient's injury (to the extent that any parties are, indeed, liable) may be difficult to determine, such as whether the failure lay with the on-site emergency room physician to order the proper study, with the teleradiologist who failed to properly interpret the symptoms, or with the on-site physician performing "overreads" on the study the next day who reads the image the same way as the teleradiologist.

6. Contractual Issues

The use of offshore outsourcing raises a range of legal issues for both administrative and clinical services, as discussed above. For the U.S.-based entities contracting with offshore service providers, the first consideration is to evaluate the risks involved in such a transaction and determining whether they are offset by the potential advantages offered by overseas services. Once the decision has been made to proceed with engaging an overseas services provider, the

[96] Shicheng Guo, at 524.

primary line of defense for the U.S.-based entity will be effective contract drafting. Towards this end, several sections of the contract will be of particular importance.

6.1 Indemnification

In the event that an overseas contractor's actions cause harm to the upstream entity (or entities plural, if the arrangement is a sub-contract), the upstream entity should be able to pursue indemnification against the subcontractor, including defense costs, penalties, fees, and/or fines.

Indemnification is, of course, not a panacea; an indemnification clause will not shield the upstream entity from its own liability, especially when that liability derives from statutory or regulatory obligations. By design, indemnification is simply meant to require the indemnifying party to stand good for any harms it causes that redound to the indemnified party.

Consider the following sample language:

> *Indemnification. [Overseas Contractor] shall indemnify and hold [U.S. Entity] harmless, including its respective directors, officers, employees and agents, from and against any and all costs, losses, damages, judgments, expenses and liabilities (including but not limited to reasonable attorneys' fees, court costs, and punitive damages) caused by or incurred as a result of [Overseas Contractor]'s breaches of any of the representations, warranties herein or acts or omissions in the performance of any of [Overseas Contractor]'s duties hereunder.*

The language above will permit the U.S. Entity to oblige the Overseas Contractor to repay a broad range of possible expenses to the U.S. Entity. The clause is worded broadly by design, to afford the U.S. Entity greater protection. This consideration underlies the use of "acts or omissions" in the drafting, rather than, for example, "negligence."

It is inadvisable to use "negligence" as a triggering mechanism for the Overseas Contractor's duty to indemnify, given that (1) it is a more narrow standard than "acts or omissions," and (2) many of the statutory and regulatory obligations that the U.S. Entity may have – and which it desires to extend to the Overseas Contractor – do not turn on a negligence

standard. For example, although one could argue that many parties that violate HIPAA have engaged in negligence (otherwise the HIPAA violation would never have occurred), the HIPAA Privacy, Security, and Breach Notification Rules do not require *negligence* by the covered entity or business associate; they simply require a failure – even one made in good faith – to comply with the regulatory requirements.[97]

The above language also does not include "alleged" acts or omissions, although it is an option for the drafting party to include such language. It is this author's view that tying indemnification to "alleged acts or omissions" is likely to be rejected by the indemnifying party. There are arguments both for and against the inclusion of such language. From the indemnified party's perspective, it may still incur expenses even if it is ultimately demonstrated that the indemnifying party's acts or omissions cannot be proven. From the indemnifying party's perspective, however, it may seem unfair that the mere allegation of a third party, even if ultimately proven false, could require the indemnifying party to pay the indemnified party's expenses. Rather than engage in such debates, actual "acts or omissions" are likely sufficient to protect the indemnified party in most cases.

Another benefit of indemnification can be its deterrent effect; its presence may inspire an overseas contractor to take contractually obligated compliance efforts more seriously than it might without an indemnification clause in the agreement. If the contractor is aware that the U.S.-based entity may demand that the contractor cover its costs for defending itself for the

[97] It is true that the OCR will often use its own enforcement discretion in determining when and how harshly to punish a covered entity or business associate that violates HIPAA, and that OCR may take into account the good faith efforts of such a party in attempting to comply with HIPAA, even if it falls short. Likewise, compliance failures where the covered entity or business associate makes a genuine effort to rectify the situation may convince the OCR to be lenient. However, none of this is required, and the underlying fact remains: a violation of HIPAA does not take into account whether the violating party was negligent.

contractor's actions or omissions, in addition to any further penalties or damages imposed upon the U.S.-based entity, the contractor may be more vigilant about its own compliance efforts.

6.2 Policies and Procedures

As a general matter, U.S.-based entities will need to impose upon overseas contractors and subcontractors obligations with which the U.S.-based entity must comply, such as compliance with HIPAA and other privacy laws and regulations, and/or compliance with state licensure laws. But simply including in the contract a duty for the overseas services provider to, for example, "comply with the terms of the Health Insurance Portability and Accountability Act of 1996 and its regulations"[98] does not go far enough. Because overseas providers may not be familiar with the specific requirements of U.S. laws – either at the federal or state level – it is essential for any U.S.-based party contracting with such an overseas provider to, at the very least, obtain and review copies of the overseas provider's policies and procedures. Ideally, this should be done prior to signing, and the overseas provider should state in the agreement[99] that it has provided the U.S.-based entity with the most current copy of such policies and procedures before execution. Consider the following sample language:

> *"[Overseas Contractor] hereby represents and warrants to [U.S.-based Entity] that it has, prior to the execution of this Agreement, provided [U.S.-based Entity] with a copy of [Overseas Contractor]'s policies and procedures for [specific U.S. law or policy] in place at the time of execution of this Agreement, attached hereto and incorporated by reference herein as Exhibit A. [Overseas Contractor] shall further notify [U.S.-based Entity] of any material changes to such policies and procedures, and shall provide a copy of such changes to [U.S.-based Entity] for its review, prior to any such changes taking effect. [U.S.-based Entity] may object to any such change and, if [Overseas Contractor] does not honor such objection, then [U.S.-based Entity] may terminate this Agreement immediately upon notice in accordance with [the applicable termination clause within the Agreement]."*

[98] And with any business associate agreement, as necessary.

[99] Such as in a representation or warranty, as discussed at 6.3 below.

Incorporating the policies and procedures as an exhibit to the agreement may be helpful for the U.S.-based entity for multiple reasons. First, it ensures that both parties were clear, at the time of signing, about which version of the policies and procedures was in effect, establishing a record of the actual meeting of the minds between the parties with respect to these policies and procedures. Second, by incorporating the policies and procedures as an exhibit, the U.S.-based entity also creates a record of its own attempts at ensuring compliance. By requesting not only a copy of the policies and procedures, but copies of any proposed alterations to them prior to the alterations taking effect, the U.S.-based company is taking a proactive approach towards ensuring that its contracting partner is meeting the standards set out by U.S. law and regulation. This is especially helpful with respect to HIPAA compliance, since actually having policies and procedures to "prevent, detect, contain, and correct security violations" is required by the Security Rule.[100] Moreover, the requirement is not that dissimilar from a common contractual provision that appears in business associate agreements, whereby a covered entity is required to notify the business associate of changes to the covered entity's notice of privacy practices. Obtaining and reviewing such policies and procedures in advance can also serve as a form of due diligence by the U.S.-based entity. If, after review of the policies and procedures, the U.S.-based entity is concerned that the overseas contractor has inadequate protections in place or does not take compliance seriously enough, that entity may choose to abandon the relationship and refuse to sign any agreement.

The sample language also permits the U.S.-based entity to terminate the agreement if it objects to a proposed change to the policies and procedures. For a U.S.-based health care

[100] 45 CFR § 164.308.

provider sharing PHI overseas, such a clause can be essential. Consider a scenario in which a large physician group decides to outsource its billing and collections overseas to a company located in another country. As part of the arrangement, the U.S.-based group uses the sample language above (or language to that effect). The overseas contractor, in an effort to improve its productivity and expand its network of potential billers and coders, alters its policies and procedures to permit its workers to work from home, including the use of removable electronic media (e.g., thumb drives, external hard drives, etc.) but does not require the use of encryption for such devices, since it believes encryption is too expensive. The U.S.-based entity objects to the policy change, but the overseas company refuses to relent. A clause like the sample language above would permit the U.S.-based company to terminate the agreement immediately without breaching, thereby protecting the U.S.-based company's PHI.

6.3 Representations and Warranties

For contracts with overseas service providers, representations and warranties will be essential. As with the language above regarding policies and procedures, such language can serve a dual role of both (1) ensuring the overseas contractor's compliance with U.S. legal and regulatory requirements, and (2) demonstrating the U.S.-based entity's own efforts to ensure its own compliance.

Any contract involving the performance of clinical services by overseas entities should include representations and warranties that the individuals performing clinical services are appropriately licensed, certified, or otherwise qualified to perform the services, and shall meet any requirements for professional liability insurance. The representations and warranties should also require the overseas contractor to provide proof of such qualifications upon request by the U.S.-based entity. The U.S.-based entity should then follow through and request and review

such documentation. Doing so will help the U.S.-based entity protect itself for compliance purposes, and will also serve as a form of due diligence.

Consider the following sample language:

> *"[Overseas Contractor] represents and warrants that all personnel providing the [clinical/professional services] shall have and maintain a license to practice [profession(s)] in the state of [State] and board certification in [specialty], and shall have and maintain professional liability insurance in such minimum amounts as required under the laws of the state of [State], but in no event any less than [$1 million per occurrence and $3 million in the aggregate], as well as any necessary extended reporting insurance. [Overseas Contractor] shall provide to [U.S.-based Entity] a copy of such licensure and insurance certificates upon request."*

The above language is straightforward and largely speaks for itself. The U.S.-based entity may request copies of documentation in support of the overseas contractor's representation and warranty that their clinical personnel will be appropriately licensed and insured. If the U.S.-based entity fails to follow through, it may face its own exposure if the overseas contractor uses unlicensed or uncertified individuals and (for example) a patient is injured as a result, or the services violate a payor requirement that results in a demand for a repayment.

Similar requirements can be applied to non-clinical services. For example, the clause above could be revised to read as follows for an overseas billing and collection agreement:

> *"[Overseas Contractor] represents and warrants that all personnel providing the [billing and collection] services shall be certified as [U.S.-based professional coder certification entity]. [Overseas Contractor] further represents and warrants that it shall have and maintain general liability insurance in amounts not less than [$1 million per occurrence and $3 million in the aggregate]. [Overseas Contractor] shall provide to [U.S.-based Entity] copies of the certification documents for all administrative personnel and insurance certificates upon request."*

Separate from issues of personnel qualification and evidence of insurance, as noted above, U.S.-based entities should consider further requiring that overseas contractors represent and warrant that they have provided the U.S.-based entity with current copies of their relevant policies and procedures, and that they will provide notice of any updates to such policies and

procedures before they are implemented. In addition to this, U.S.-based entities may want to require that overseas contractors represent and warrant that they will follow their own policies and procedures. It is not enough to simply have such policies in place; the parties must actually operate in accordance with those policies. It is bad to have no policies and procedures in place. It is worse to have them and then ignore them. U.S.-based entities should also consider requiring that overseas contractors represent and warrant that they will comply with applicable U.S. laws, including HIPAA.

Requiring that overseas contractors represent and warrant these issues is important for U.S.-based entities. Because representations and warranties act as an inducement to the non-representing party to enter into the agreement, if they are breached and the non-representing party is harmed as a result, the non-representing party may be able to obtain punitive damages in addition to actual damages. When dealing with overseas companies that may not be as familiar with the U.S.' health care laws and regulations, this may be essential to protect U.S.-based companies. Additionally, assuming the overseas entity understands the significance of representations and warranties in U.S. contract law, the clause may serve to inspire greater efforts at compliance, since the overseas entity will be on notice that failures on their part could lead to much harsher penalties than regular damages.

6.4 Auditing Rights

In addition to the above, U.S.-based entities should carefully consider including in their agreements with overseas contractors provisions that grant them the right to conduct periodic audits of the overseas contractor. U.S.-based entities should consider requesting copies of the overseas entity's policies and procedures to ensure the privacy and security of PHI (and any other relevant compliance-related policies and procedures), copies of licensure or other required

certification for the overseas' entity's personnel (especially when such licensure or certification is a representation and warranty), copies of insurance certificates, and randomly selected vendor contracts. Likewise, U.S.-based entities should request inventories of their ePHI, which describe where and how such information is stored. This should include any documentation to support the security standards to which the overseas entity's software is held, especially if such standards comply with HIPAA requirements.

As a practical matter, such audits will have to be performed remotely (often referred to as a "desk audit"). U.S.-based entities will likely have to strike a balance in drafting contractual terms for such audits between two competing goals: the U.S.-based entity's desire to ensure that the information produced in the audit is reliable (which could be demonstrated by the speed with which it is produced), and the overseas entity's desire to avoid unnecessary disruptions to its operations (which could be achieved by having advance notice of requests for documentation or other audit materials). This will require the parties to negotiate an appropriate notice period whereby the U.S.-based entity can notify the overseas entity that it must produce requested documentation or provide remote access as applicable. The U.S.-based entity will want this time period to be as short as possible to ensure that the overseas entity is not simply crafting documentation on the fly, and is actually adhering to its obligations on an ongoing basis. The overseas entity will want to ensure that the U.S.-based entity's request does not unduly interfere with its regular operations. Ideally, an overseas entity will produce documentation within a short timeframe, such as ten business days or fewer. The more time they have to respond, the less spontaneous the audits can be, and the less certainty the U.S.-based entity will have that the overseas entity is conducting itself appropriately. That said, gathering and transmitting

documentation may be reasonably expected to take a few days, depending on the nature of the documentation.

Regardless, the underlying duty to permit and cooperate with such audits is not unreasonable and should not be controversial. The U.S.-based entity is likely to find itself in the crosshairs of any enforcement action or lawsuit in the event that things go awry. Even with contractual language that permits the U.S.-based entity to obtain indemnification or punitive damages (e.g., through breaches of representations and warranties by the overseas entity), securing a judgment against the overseas entity may prove difficult. Moreover, both indemnification and punitive damages are entirely remedial; the horses, by this point, have already fled the barn. The purpose of ongoing audit rights, however, is *preventative*, designed to catch potential problems before they occur, and thereby better protect the U.S.-based entity. Ideally, by including such language, the U.S.-based entity will be forewarned as to potential problems and either be able to correct them, or terminate the agreement.

7. Conclusion

It is unlikely that overseas outsourcing as a phenomenon within the health care industry will disappear over time. Health care providers face budgetary pressures and will look for ways to alleviate those costs. If overseas outsourcing can provide the savings they need, health care providers will try to make such arrangements work, even if they also present difficulties that must be overcome. Moreover, the full, long-term impact of the COVID-19 pandemic on the health care industry is as yet unknown. In addition to the financial impact across the economy – both within the United States and worldwide – COVID-19 forced many states and health care payors to reevaluate the viability of telemedicine and remotely provided services, both clinical and administrative. Many barriers that had previously limited the widespread use of

telemedicine have been removed without the world spinning off of its axis. Although it is likely that some of these barriers will return (e.g., state licensure processes will likely tighten up again when the pandemic abates), other barriers may well be left by the wayside as they are determined to no longer be necessary. In the midst of all of this, health care providers will continue to use outsourced services, many of which will be provided from overseas. As a result, attorneys who represent them will need to help them navigate these waters, through a combination of careful negotiation of state law issues, HIPAA considerations, and especially contractual provisions.