Provider Beware: Potential Pitfalls of Fraud in Government Telehealth Programs
(American Bar Association Health eSource, May 15, 2020)

By Darryl Landahl, Esq. Amanda Hutson, Esq., and Ishra Solieman

---

The utilization of telehealth[1] services has dramatically increased in recent years with improvements in technology and increased provider and patient comfort with the delivery of healthcare through virtual means. Almost certainly, acceptance of and comfort with telehealth - by providers, patients and regulators – will now increase exponentially as a result of the COVID-19 pandemic.

Among rural Medicare beneficiaries, the number of telehealth visits increased from 7,015 in 2004 to 107,955 in 2013, an increase of over 1,000 percent, and continues to rise.[2] While the statistics on utilization vary based on the reporting organization, FAIR Health reported[3] that from 2014 to 2018, the use of non-hospital-based provider-to-patient telehealth grew 1,393 percent, from 0.0007 percent to 0.104 percent of all medical claim lines.[4] Claim lines related to any type of telehealth grew 624 percent.[5] The American Medical Association (AMA) presented national estimates on the overall use of telehealth in December 2018, reflecting that at least 15 percent of physicians worked in practices that used telehealth for patient interaction.[6] This number was significantly higher within certain specialties, with 39.5 percent of radiologists, 27.8 percent of psychiatrists, and 24.1 percent of cardiologists reporting utilization of telehealth for patient interactions.[7] And according to a recent American Hospital Association (AHA) survey, more than 76 percent of U.S. hospitals connect with patients and consulting practitioners through the use of video and other technology.[8] The survey

---

[1] The Health Resources and Services Administration of the U.S. Department of Health and Human Services defines telehealth as the use of electronic information and telecommunications technologies to support and promote long-distance clinical healthcare, patient and professional health-related education, public health and health administration. Telehealth is different from telemedicine because it refers to a broader scope of remote healthcare services than telemedicine. While telemedicine refers specifically to remote clinical services, telehealth can refer to remote non-clinical services. This article uses the term `telehealth" when referring to both telehealth and telemedicine services.

[2] Mehrotra, A., Jena, A.B., Busch, A.B., Souza, .J, Uscher-Pines, L, & Landon, B.E., Utilization of Telemedicine Among Rural Medicare Beneficiaries, *JAMA*, 2016;315 (18)2015-2016. doi:10.1001/jama.20162186.

[3] FAIR Health, A Multilayered Analysis of Telehealth, A FAIR Health White Paper (July 2019) at 7. FAIR Health is an independent, national nonprofit organization known for providing neutral information on healthcare costs and health coverage. FAIR Health collects healthcare bills from health insurers around the country and currently holds a database of more than 30 billion claims.

[4] FAIR Health analyzed data in its repository of over 29 billion private healthcare claim records and compiled them into "claim lines."

[5] FAIR Health, *supra* n. 3.

[6] AMA, AMA Offers First National Estimate of Telemedicine Use by Physicians (December 2018), https://www.ama-assn.org/press-center/press-releases/ama-offers-first-national-estimatetelemedicine-use-physicians.

[7] *Id*.

[8] AHA, AHA Annual Survey IT Supplement (2011-2018), https://www.ahadatacom.

also found that more than half of those hospitals have implemented remote patient monitoring capabilities.[9]

This increase in the use of telehealth has, of course, increased the amount of federal program reimbursement for such services. The Department of Health and Human Services Office of Inspector General (OIG) stated that Medicare paid a total of $17.6 million for telehealth services in 2015, compared to just $61,302 in 2001.[10]

While the growing availability of telehealth services facilitates care for patients who otherwise might not have adequate access to providers, it also comes with an increased risk of fraud and abuse.

Most government healthcare programs cover some form of telehealth services, including Medicare, state Medicaid programs, Veterans Affairs, TRICARE, and the Indian Health Service. As providers consider whether to offer telehealth services to beneficiaries of these programs, it is vital that they are aware of and understand the potential ways federal fraud and abuse laws might be violated – often unintentionally. Among the federal laws implicated by the offering of telehealth services are the Civil Monetary Penalties Law (CMP),[11] the Anti-Kickback Statute (AKS),[12] the Stark Law,[13] and the False Claims Act (FCA).[14]

Common examples of telehealth arrangements that could potentially violate one or more of these laws include providing telehealth-related equipment to organizations or physicians who are referral sources, and billing for telehealth services that were not appropriately supervised or that were not rendered in compliance with state law licensure and scope of practice laws. In recognition of the risk of abuse that is latent in telehealth, the OIG pursued its first ever FCA enforcement action against a telehealth provider in 2016, signaling to telehealth practitioners nationwide that the OIG is serious about prosecuting attempts to defraud federal and state healthcare programs through the provision of telehealth services.[15] Since then, enforcement of fraud in government telehealth programs has increased tenfold, when comparing the number of DOJ press releases relating to telehealth fraud prosecutions each year.

Summary of Fraud and Abuse Laws Applicable to Telehealth Services

The Civil Monetary Penalties Law

The CMP authorizes the U.S. Secretary of Health and Human Services to impose civil monetary penalties against any person that offers or gives remuneration to any

[9] *Id*.
[10] OIG, CMS Paid Practitioners for Telehealth Services That Did Not Meet Medicare Requirements (Apr. 2018).
[11] 42 U.S.C. §1320a-7a.
[12] 42 U.S.C. §1320a-7b(b).
[13] 42 U.S.C. §1395nn.
[14] 31 U.S.C. §3729.
[15] DOJ, Danbury Physician and Mental Health Practice Pay $36,000 to Settle False Claims Act Allegations (July 2016), https://www..justice.goviusao-ct/pridanbury-physician-and-mental-health-practice-pay-36000-settle-false-claims-act.

beneficiary of a federal healthcare program when the person knows or should know the remuneration is likely to influence the beneficiary's selection of the provider for Medicare or Medicaid reimbursable items or services - often referred to as the "Beneficiary Inducement CMP"[16] The CMP defines "remuneration" for purposes of the Beneficiary Inducement CMP as including "transfers of items or services for free or for other than fair market value."[17] In the telehealth context, the Beneficiary Inducement CMP may be triggered by seemingly innocuous encounters – for example, when a provider offers a patient a free remote monitoring device or an application that helps track medical data.

There are a few exceptions to the Beneficiary Inducement CMP that telehealth arrangements may fall under. For example, the Promotes Access to Care Exception" provides that the "remuneration must (1) improve a beneficiary's ability to obtain items and services payable by Medicare or Medicaid and (2) pose a low risk of harm to Medicare and Medicaid beneficiaries and the Medicare and Medicaid programs."[18] An arrangement must meet specific criteria, as outlined by the OIG, in order to qualify under this exception.[19] Another exception to the Beneficiary Inducement CMP is the "Financial Need Exception," which provides that the offer or transfer of items or services for free or less than fair market value does not constitute "remuneration" if: (1) the items or services aren't offered as part of advertising or solicitation; (2) the items or services are not tied to the provision of other services reimbursed by Medicare or Medicaid; (3) there is a reasonable connection between the items or services and the medical care of the individual; and (4) the items or services are provided only after a good faith determination is made that the individual is in financial need.[20]

If a telehealth arrangement does not meet the requirements of an exception to the CMP, the OIG may determine in an exercise of its discretion whether it will pursue an action against the provider. This exercise of discretion is generally based on the OIG's analysis of the risk that an arrangement offering free or reduced items or services will influence patients to choose the provider for federally reimbursable items or services in the future, the apparent underlying purpose of the arrangement, and any safeguards the provider has put in place to reduce the risk of abuse.

The Anti-Kickback Statute

Under the AKS, it is a criminal offense to knowingly and willfully offer, pay, solicit, or receive, directly or indirectly, any remuneration in return for referring, furnishing, arranging, or recommending items or services reimbursable by any federal healthcare program.[21] Some telehealth arrangements can potentially violate the AKS if not properly structured and defined. Indeed, the OIG has issued numerous advisory opinions discussing the applicability of the AKS to various types of telehealth arrangements.

[16] 42 U.S.C. §1320a-7a.
[17] 42 U.S.C. §1320a-7a(i)(6).
[18] 42 U.S.C. §1320a-7a(i)(6)(F); OIG, Advisory Op. No.19-03 (March 1, 2019) at 7.
[19] OIG, Advisory Op. No.19-03 (Mar. 1, 2019) at 7.
[20] 42 U.S.C. §1320a-7a(i)(6)(H).
[21] 42 U.S.C. §1320a-7b(b).

Common themes emerge in five of these OIG advisory opinions:[22] (1) the use of telehealth services is unlikely to increase costs under federal programs beyond what is paid for the same services rendered in person, and (2) increased utilization of telehealth can yield significant public benefits, but (3) free or discounted telehealth services and equipment are considered forms of remuneration.

These themes are embodied in the example of a large hospital system that leases telehealth equipment at a discounted rate (or for free) to rural medical practices. In this situation, the hospital system could be in violation of the AKS (and other fraud and abuse laws) for providing equipment below fair market value and would therefore need to structure the telehealth equipment lease in a mariner that fits an applicable safe harbor in order to mitigate any potential liability.[23]

The OIG addressed this type of arrangement in a 2018 OIG advisory opinion that responded to an inquiry from a nonprofit federally qualified health center that planned to use state funds designated for HIV prevention efforts to offer free telehealth equipment and services to a county clinic providing HIV testing and treatment.[24] The OIG noted that the county clinic could possibly serve as a referral source to the health center and would receive remuneration in the form of telehealth items and services in violation of the AKS.[25] Despite this, the OIG advised that it would not pursue an enforcement action against the requestor under the described arrangement because it posed a low risk of abuse. Specifically, the OIG determined that the arrangement included sufficient safeguards to prevent inappropriate patient steering did not inappropriately increase costs to federal health programs, and improved patient access to care.[26] Among the safeguards which the OIG found effective were the absence of a requirement that the county clinic refer to the provider, that the county clinic informed patients of their ability to receive care from any provider whether in-person or virtually, and that the telehealth devices did not inappropriately limit or restrict the flow of information.[27] Thus, the OIG advised that it would exercise its discretion and not pursue enforcement against the requestor even though the arrangement could potentially generate prohibited remuneration under the AKS if the requisite intent were present

The Stark Law

The Stark Law prohibits a physician from referring patients for certain designated health services payable by Medicare to an entity when the physician (or the physician's immediate family member) has a financial relationship with that entity, unless an exception applies.[28] Although there are numerous ways in which a telehealth services

[22] OIG, Advisory Op. No.11-12 (Aug. 29, 2011); OIG, Advisory Op. No. 04-07 (June 17, 2004); 01G, Advisory Op. No. 99-14 (Dec. 28,1999); OIG, Advisory Op. No.18-03 (May 21, 2018); OIG, Advisory Op. No. 98-18 (Nov. 25, 1998).
[23] For a complete listing of regulatory safe harbors and their respective requirements, *see* 42 C.F.R §1001.952.
[24] OIG, Advisory Op. No.18-03 (May 31, 2018) at 5-7.
[25] *Id*. at 6.
[26] *Id*.
[27] *Id*.
[28] 42 U.S.C. §1395nn.

arrangement could implicate the Stark Law, two common examples are referrals to organizations that provide physicians with free or discounted access to telehealth equipment or services and referrals to telehealth organizations by physicians who are financially connected to the organization, other than as an employee. Providers considering a telehealth arrangement that involves such referrals should ensure that the arrangement falls within a Stark Law exception.

The False Claims Act

The FCA creates liability for any person who knowingly submits a false claim to the government or causes another person to submit a false claim to the government, or knowingly makes a false record or statement in order to get a false claim paid by the government.[29] One source of FCA liability to which telehealth providers are particularly susceptible is non-compliance with the Medicare program's payment requirements for physician services. Failing to meet these requirements could potentially result in a violation of the FCA.

Medicare Part B pays for covered telehealth services included on the telehealth list when furnished by an interactive telecommunications system if the physician/practitioner at the distant site is licensed to furnish the service under state law to a beneficiary at an originating site.[30] An OIG report in 2018 found that approximately 30 percent of the telehealth service claims in its sample did not meet Medicare reimbursement requirements.[31] The OIG estimated that Medicare could have saved approximately $3.7 million during the audit period if practitioners had provided telehealth services in accordance with Medicare requirements.[32]

It is unclear from the OIG's findings whether these false claims were the result of intentional conduct or provider misunderstanding of the Medicare requirements applicable to telehealth services. Notwithstanding the OIG has signaled it is serious about pursuing FCA enforcement against telehealth providers that it determines have attempted to defraud federal and state healthcare programs.[33]

Recent Telehealth-Related DOJ Enforcement Activities

In September 2019, the Department of Justice (DOJ) announced one of the largest telehealth fraud schemes ever investigated and prosecuted by the federal

[29] 31 U.S.C. § 3729.
[30] 42 C.F.R § 410.78(b).
[31] OIG, CMS Paid Practitioners for Telehealth Services That Did Not Meet Medicare Requirements (Apr. 2018).
[32] *Id.*
[33] *See* DOJ, New Jersey Doctor Pleads Guilty to $13 Million Conspiracy to Defraud Medicare with Telemedicine Orders of Orthotic Braces (Sept 2019), https://www.justice.gov/opa/pr/new-jersey-doctor-pleads-guilty-13-million-conspiracy-defraud-medicare-telemedicine-orders; *see also* DOJ, Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses (Apr. 2019), haps://www..justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.

government.[34] According to allegations included in the DOJ court filings, this scheme involved defendants obtaining patients for the scheme by using an international call center that advertised to Medicare beneficiaries and "up-sold" the beneficiaries to induce them to accept numerous "free or low-cost" durable medical equipment (DME) braces, regardless of medical necessity.[35] The international call center allegedly paid illegal kickbacks and bribes to telehealth companies to obtain DME orders for these Medicare beneficiaries.[36] The telehealth companies then allegedly paid physicians to write medically unnecessary DME orders.[37] The international call center then sold the DME orders that it obtained from the telehealth companies to DME companies, which fraudulently billed Medicare.[38]

According to the DOJ, the coordinated healthcare fraud enforcement action covered seven federal districts and involved more than $800 million in losses.[39] The investigation resulted in charges against 48 defendants for their roles in submitting over $160 million in fraudulent claims, including charges against 15 physicians and other medical professionals, and another 24 who were charged for their roles in diverting opioids.[40] The action has already resulted in the guilty pleas of three corporate executives for their roles in causing the submission of over $600 million in fraudulent claims to Medicare, including the Vice President of Marketing of numerous telehealth companies and two owners of approximately 25 DME companies.[41] One of the physicians in the scheme also pled guilty for his role and agreed to pay over $7 million in restitution, as well as forfeit assets and property traceable to proceeds of the conspiracy.[42]

Less than a week later, a New Jersey physician pled guilty to a separate $13 million healthcare fraud conspiracy with telehealth companies.[43] The physician admitted that he worked for two purported telehealth companies for which he wrote medically unnecessary orders for orthotic braces for Medicare beneficiaries.[44] He admitted that he wrote the brace orders without speaking to the beneficiaries and concealed the fraud with falsified orders that stated, among other things, that he had "discussions" or

[34] DOJ, Federal Health Care Fraud Takedown in Northeastern U.S. Results in Charges Against 48 Individuals (Sept 2019), https://wwwjustice.gov/opa/prifederal-health-care-fraud-takedown-northeastern-us-results-charges-against-48-individuals.
[35] DOJ, Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses (Apr. 2019), https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.
[36] *Id.*
[37] *Id.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] DOJ, New Jersey Doctor Pleads Guilty to $13 Million Conspiracy to Defraud Medicare 25 with Telemedicine Orders of Orthotic Braces (Sept. 2019), https://wwwjustice.gov/opa/prinew-jersey-doctor-pleads-guilty-13-million-conspiracy-defraud-medicare-telemedicine-orders.
[44] *Id.*

"conversations" with the beneficiaries.[45] These cases "show that the DOJ remains laser-focused on uprooting corporate health care fraud schemes," according to a statement by Assistant Attorney General Brian A. Benczkowski of the DOD's Criminal Division.[46]

Similarly, in July 2019 an anesthesiologist was indicted by a grand jury for conspiracy to commit healthcare fraud for her alleged role in a telehealth scheme to submit fraudulent claims.[47] According to the indictment, the anesthesiologist received kickbacks from unidentified companies in exchange for writing prescriptions for DME for her telehealth patients.[48] But in fact the prescriptions were not medically necessary and were not the result of an actual doctor-patient relationship or examination.[49]

In another subset of cases, the DOJ has charged physicians with running the fraudulent schemes themselves. For instance, in *United States v. Powers*, the defendant physicians were charged for allegedly operating a scheme involving an online telehealth portal that promoted the sale of compounded medications.[50] They allegedly recruited other physicians to review patient files that the defendants falsely claimed were prepared by other qualified practitioners, and then used the reviewing physicians' identities and medical credentials to authorize the compounded medication prescriptions.[51]

While the above examples involve physicians that knowingly participated in the fraud, physicians have also found themselves at the center of enforcement actions where they were wholly unaware of the fraudulent telehealth scheme. For example, in June 2019, Florida-based telehealth company HealthRight settled a 32-count indictment.[52] The non-physicians charged in the scheme illegally obtained patients' insurance information and prescriptions for pain-relief cream and other products. Over 100 physicians unaware of the scheme but practicing via telehealth then approved the prescriptions, which the compounding pharmacies filled for substantially marked-up prices.[53] The conspirators then billed insurance companies, submitting more than $930 million in false claims.[54] The physicians who unwittingly participated in the scheme have thus far not been charged by the DOJ and are referred to in the indictment as the "defrauded doctors" who had no knowledge of the scheme.

---

[45] *Id*.
[46] *Id*.
[47] DOJ, Anesthesiologist Indicted for Alleged Role in $7 Million Telemedicine Health Care Fraud Conspiracy (July 2019), https://www.justice.gov/usao-edny/pr/anesthesioloOst-indicted-alleged-role-7-million-telemedicine-health-care-fraud.
[48] *Id*.
[49] *Id*.
[50] *United States v. Powers*, No. 8:17-cr-00077 (C.D. Cal filed June 18, 2017) at 3.
[51] *Id*.at 3-5.
[52] DOJ, Four Men and Seven Companies Indicted for Billion-Dollar Telemedicine Fraud Conspiracy, Telemedicine Company and CEO Plead Guilty in Two Fraud Schemes (Oct. 2018), https://wwwjustice.gov/opa/pr/four-men-and-seven-companies-indicted-billion-dollar-telemedicine-fraud-conspiracy.
[53] *Id*.
[54] *Id*.

Efforts to Curb Fraudulent Telehealth Activities

These enforcement actions highlight a concern that the growing utilization of telehealth technologies will create new opportunities for wrongdoers to defraud providers and patients by creating fictitious telehealth encounters, posing as patients, and deceiving physicians into ordering or prescribing unnecessary products and services. These concerns stem in significant part from the technical challenges associated with authenticating the identities of both the patients and providers involved in telehealth encounters. The telehealth provider community, through organizations such as the American Telemedicine Association (ATA), has taken steps to address these verification issues by developing guidelines and recommendations and encouraging the provider community's adoption of them into their telehealth policies and protocols.[55]

As with any fast-growing area, telehealth is particularly vulnerable to both intentional and unintentional violations of fraud and abuse laws. Moreover, the laws surrounding telehealth and its reimbursement are complex and can be confusing, and could become even more difficult to navigate during the COVID-19 pandemic.[56] The key to ensuring compliance is to learn about the pitfalls associated with these fraud and abuse laws and to implement best practices for minimizing the risk of a violation. Such best practices should include a robust compliance program that incorporates the ATA guidelines and protocols for patient identification and authentication, encourages internal reporting of suspected telehealth fraud in particular, and includes training and educational programs for practitioners and staff on appropriate telehealth documentation and billing practices. If the recent wave of government crackdown on telehealth fraud is any indication, compliance officers of healthcare organizations should pay careful attention to their delivery of telehealth services.

Proposed Changes to Stark, AKS, and CMP Related to Telehealth

On October 9, 2019, the Department of Health and Human Services (HHS) published proposed changes to the Stark Law,[57] AKS,[58] and CMP[59] regulations in an effort to provide greater certainty for healthcare providers participating in value-based arrangements and providing coordinated care for patients.[60] This historic reform

---

[55] *See* Am. Telemedicine Assn, Core Operational Guidelines for Telehealth Services Involving Provider-Patient Interactions (May 2014). These guidelines provide guidance on educating patients about telehealth treatment, best practices for verification of patient/provider identity and service delivery location, guidance related to mobile devices and services delivered to patients in non-facility settings and various guidelines on privacy and security requirements. These include building session and participant limits into videoconferencing software, ensuring safeguards to prevent other individuals from overhearing physician-patient conversations, and documenting physician and patient locations.

[56] This is especially true since CMS and the OIG created waivers for telehealth pertaining to the COVID-19 public health emergency. *See* https://www.cms.gov/newsroom/fact-sheets/medicare-telemedicine-health-care-40 provider-fact-sheet; *see also* https://oig.hhs.gov/fraud/docs/alertsandbulletins/2020/policy-telehealth-2020.pdf.

[57] 42 U.S.C. §1395nn.

[58] 42 U.S.C. §1320a-7b(b).

[59] 42 U.S.C. §1320a-7a(a)(5).

[60] HHS, HHS Proposes Stark Law and And-Kickback Statute Reforms to Support Value-Based and Coordinated Care (Oct. 2019), https://www.hhs.gov/about/news/2019/10/09/hIts-proposes-stark-law-anti-kickback-statute-reforms.html.

includes changes that affect the provision of telehealth services and could potentially ease the compliance burden on telehealth providers. Along with the proposed changes, HHS provided a list of example arrangements that do not fit under existing AKS safe harbors and CMP and Stark exceptions but that could potentially be protected by the new proposals.[61] Most of these examples included telehealth-related services and technologies, such as: hospitals sharing data analytics services with primary care physicians; entities providing patients with free post-discharge monitoring technology or smart pillboxes with automatic physician alerts; and providers furnishing patients with technology capable of real-time interactive communication between patient and physician.[62]

The proposed changes would provide additional guidance on several key requirements that must be met in order for telehealth providers to comply with fraud and abuse laws. Additionally, the proposed rules include exceptions that would provide new flexibility for certain arrangements — such as donations of certain cybersecurity technologies that safeguard the integrity of the healthcare ecosystem — regardless of whether the parties operate in a fee-for-service or value-based payment system.[63] Indeed, both the proposed changes to Stark and AKS regulations include modifications to their respective exceptions and safe harbors for the donation of electronic health record technology and associated services.[64]

Stakeholders had the opportunity to provide comments to HHS on the proposed changes through December 31, 2019.[65] Healthcare providers should continue to monitor these changes with particular attention to the telehealth implications, as they likely will significantly alter the applicable laws and best practices for minimizing the risk of a violation.

Conclusion

Although increased utilization of telehealth services has the potential to significantly lower healthcare costs and improve the health outcomes of patients, these benefits unfortunately increase the risk of fraud and abuse in government programs. New regulations being considered this year may help clarify the regulations applicable to telehealth and, in turn, potentially make telehealth easier for providers to properly implement. Moreover, the recent increase in telehealth utilization due to the COVID-19 pandemic may help provide insights to guide telehealth use in the future. It is incumbent on providers and their counsel to understand the fraud and abuse laws implicated by the use of telehealth, and give appropriate consideration to structuring relationships involving telehealth in order to mitigate any potential liability.

[61] *Id.*
[62] *Id.*
[63] 84 Fed. Reg. 55766; 84 Fed. Reg. 55694.
[64] *Id.*
[65] *Id.*

About the Authors

Darryl Landahl advises healthcare providers in structuring complex healthcare transactions and relationships, and has represented some of the largest healthcare companies in the United States. He has substantial experience representing healthcare industry clients on a state and national level in regulatory, transactional and litigation matters. He has particular expertise in risk-based and other alternative payment models, and in developing IPAs and provider networks. He also has extensive experience advising clients on federal and state fraud and abuse laws, corporate practice of medicine restrictions, and operational issues. He may be reached at dlandahl@bhfs.com.

Amanda Hutson focuses her practice on regulatory, litigation and corporate matters in the healthcare sector, drawing upon her in-house experience and wealth of industry knowledge. Prior to joining Brownstein, Ms. Hutson worked as a legal department intern at one of the largest non-profit healthcare systems in the United States, working in the areas of fraud and abuse, HIPAA, nonprofit regulation, licensure, and operations. She may be reached at ahutson@bhfs.com.

Ishra Solieman advises healthcare providers and organizations on an array of regulatory compliance issues, and has particular experience with managing provider self-audits and self-disclosures associated with potential fraud and abuse claims, compliance with state licensing provisions, the development and implementation of comprehensive HIPAA policies and procedures, and assisting clients in the management of the regulatory issues that inevitably arise in a healthcare organization's day-to-day operations. Ms. Solieman's previous experience with healthcare litigation informs how she strategizes with provider clients on potential disputes in keeping with their goals. She may be reached at isolieman@bhfs.com.