Practical Guidance

AI in Healthcare: Cautions and Considerations of a Healthcare Revolution

A Practical Guidance® Practice Note by Sara Shanti, Phil Kim, Christopher Rundell, Arushi Pandya, and Elfin Noce, Sheppard Mullin

Sara Shanti
Sheppard Mullin

Phil Kim
Sheppard Mullin

Christopher Rundell
Sheppard Mullin

Arushi Pandya
Sheppard Mullin

Elfin Noce
Sheppard Mullin

The use of generative artificial intelligence (AI) and machine learning (ML) in healthcare recently has been developing at a fanatical and fascinating pace. Because the consequences of such technology are yet to be fully understood, thoughtful consideration of its use by industry stakeholders and users is necessary, especially with respect to the legal implications within the healthcare industry. This practice note discusses AI's development in healthcare and federal and state efforts to regulate its use. It provides health law practitioners with an overview of the legal considerations associated with AI's use in healthcare, including data privacy, corporate practice of medicine, provider licensing, reimbursement, intellectual property, and research. It concludes with a discussion of the ethical considerations involved with AI in healthcare and considerations for protections against potential liability.

This practice note is organized into the following topics:

- AI's Development in the United States and Certain Foreign Jurisdictions
- Existing Legal Framework of AI Regulation in the United States
- AI Regulatory Considerations in U.S. Healthcare
- Ethical Considerations of AI Use in Healthcare
- Protecting against Potential Healthcare AI Liabilities
- Conclusion – Successful AI Requires Sophisticated Regulation and Regulatory Counsel

For an overview of current practical guidance on generative AI, ChatGPT, and similar tools, see Generative Artificial Intelligence (AI) Resource Kit.

To follow legislative developments related to ChatGPT and generative AI, including those related to healthcare, see ChatGPT Draws State Lawmakers' Attention to AI.

AI's Development in the United States and Certain Foreign Jurisdictions

Although AI can be described simply as the engineering and science of making intelligent machines, its effects are much more complex. ML is a subset of AI focused on how to improve computer operations based on informed actions and statistics. While AI programming has been in existence for decades, the recent developments in generative AI have been transformative in mainstream use. Accelerated growth in healthcare can be attributed, at least in part, to the COVID-19 Public Health Emergency (PHE) when digital healthcare, including products driven by AI, emerged as a marketable means to accessible care.

Pre- and post-PHE, the United States has been a premier healthcare leader with breakthrough innovations and research, and this continues to be the case with AI's evolution. However, the current barren regulatory landscape has cast a unique shadow over AI's potential, which is particularly significant in light of an aging population, high Medicaid and Children's Health Insurance Program enrollment—growing 29.8% from February 2020 to December 2022—and multiple ongoing epidemics in mental health and substance abuse. Considering this healthcare climate, AI as a regulated and tamed tool has an incredible opportunity in history with its unique ability to renovate the health and wellness not only of the nation, but the entire global population, at a pivotal point in human history.

Such optimism stands in stark contrast to warnings about AI's potential to harm or mislead. In fact, the World Health Organization (WHO), which issued the Ethics & Governance of Artificial Intelligence for Health in 2021, recently called for caution to be exercised as "the data used to train AI may be biased, generating misleading or inaccurate information that could pose risks to health, equity and inclusiveness." While international bodies, like the European Union, have been actively monitoring and pushing for limitations on AI for years, to date, the United States has virtually allowed the industry to regulate itself. Without swift action, de facto legal regimes for AI may be established outside of the United States, most significantly in China, if only due to the size of its population base. This is notable, as is the lack of experience by federally elected officials and staff in the crucial arena of computer science and law, coupled with the fact that Congress has been notoriously adverse to imposing sweeping limitations on technology companies. The United States has a tremendous opportunity to grow and lead in this arena. Alternatively, many experts strongly believe the role of governing AI must be a global collaboration with international monitoring, similar to how the nuclear field is regulated. While AI now has legislators' attention and future regulation is ultimately expected, stakeholders are hyper-aware of the implications of further delay.

Deaf to legislation battles, AI/ML in healthcare has advanced in a broad range of applications, from innovations in identifying acute health episodes and improving personalization of care and treatment plans, to pharmaceutical development and isolation and self-harm prevention. Understanding that AI is constantly evolving, this practice note focuses on the legal considerations of AI in healthcare in the United States that can be applied alongside regulatory developments to support protective and successful implementation.

Existing Legal Framework of AI Regulation in the United States

Currently, no comprehensive federal framework to regulate AI/ML exists. The White House's Blueprint for an AI Bill of Rights does offer high-level direction in the design, deployment, and use of automated systems to prioritize civil rights and democratic values, a number of federal agencies have issued high-level guidance or statements, and Congress is taking steps to educate itself, including through hearings with stakeholders and technology executives; however, material and standardized safeguards have yet to be established. In contrast, certain states are actively developing and implementing laws to oversee the development and deployment of AI that impacts healthcare. For example, the California Consumer Privacy Act (CCPA) provides consumers with rights to opt out of automated decision-making technology. Illinois' proposed Data Privacy and Protection Act would regulate the collection and processing of personal information and the use of so-called covered algorithms, which include computational processes utilizing AI/ML. Approximately half of the country's states already have pending or enacted AI legislation.

Stakeholder and industry groups are also actively releasing guidance, despite the lack of enforceability, which materially limits its implementation. For instance, in order to align on health-related AI standards in a patient-centric manner, the Coalition for Health AI (CHAI) released a Blueprint For Trustworthy AI Implementation Guidance and Assurance

for Healthcare. The American Medical Association (AMA) has similarly published Trustworthy Augmented Intelligence in Health Care, a literature review of existing guidance, in order to develop actionable guardrails for trustworthy AI in healthcare.

AI Regulatory Considerations in U.S. Healthcare

At minimum, industry actors should consider the full array of healthcare regulatory and legal issues when creating or using AI/ML products, including those described herein.

Data Privacy

The privacy rights of patients and users are a tremendous consideration at the crux of AI/ML. Consumer and health information privacy laws may be implicated at both the federal and state level with regard to the access, sharing, and use of protected health information (PHI) and personally identifiable information (PII) with AI/ML. Generally, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, limits the ability of certain health entities to share PHI unless an exception applies, and specifically prohibits the sale and commercialization of PHI. In addition, many state data privacy laws are broader and more comprehensive than HIPAA, including CCPA and Washington's recently enacted My Health My Data Act, 2023 Wash. Advance Legis. Serv., ch. 191. Such laws may necessitate authorization, consent, notice, or proper anonymization of data prior to its transfer or use. Further, certain sensitive data, such as mental health, reproductive health, and substance use disorder information, genetic information, and healthcare records of minors are subject to more aggressive restrictions. As such, in assessing AI/ML models or algorithms, it is critical to determine whether PHI, PII, or other sensitive data is regulated and whether consent, notice, and/or other preconditions must be met prior to accessing, disclosing, or transmitting data in AI/ML products.

Data Assets and Rights

With the development of AI/ML, data already collected by healthcare providers becomes a valuable asset that can be used to improve the quality of care for patient populations, and it can also be monetized with further use cases. In order for AI/ML to provide quality results, relevant and high-quality data tailored to the task at hand is imperative. Quality patient data collected at the provider level can be used to improve AI/ML, ultimately resulting in higher-quality outputs. This data can also be monetized through licensure to other companies looking for quality data to train their own AI/ML models. There should be a disciplined approach when allowing third parties or vendors access to this data, as these third parties often request broad rights to use the data to improve their services. Agreements should be carefully crafted to clearly retain all ownership rights in its data for its users, while also providing the relevant third party a limited license to use such data as desired.

Data Commercialization

Relatedly, caution should be exercised where an AI/ML health product does not have a monetary cost for its use. In some instances, developers of allegedly free AI/ML products are compensated via the use of valuable client data entered into the product. Essentially, a user may be trading data holding value and, in effect, privacy of the data subjects, for the use of the product. The terms of use and privacy policies associated with such products should be closely reviewed to determine the data rights that may be exchanged for the use of an AI/ML product.

The commercial and legal stakes are specifically high with regard to the use of data in AI/ML training. Use of data in a manner that violates federal or state data privacy laws can be potentially catastrophic for an AI/ML product and patient welfare. The developer of the AI/ML model or algorithm could be required to unwind the improperly used data from the AI/ML, which is a complex, near-impossible task, or else destroy the AI/ML models or algorithms that were trained with data that was not properly licensed or obtained, as the FTC has required for certain algorithms trained with improperly used data.

Corporate Practice of Medicine

Generally, the corporate practice of medicine doctrine (CPOM) prohibits the practice of medicine by a corporation, including by employment of licensed healthcare providers (physicians, and in some states other licensed healthcare providers), other than by a professional corporation owned by individuals duly licensed to practice the profession. The public policy rationale behind CPOM is that clinical decision-making should be left to duly licensed professionals, and not be unduly influenced by unlicensed persons or corporations. Not all states have CPOM restrictions, and CPOM laws vary widely state-to-state.

Under existing doctrines, CPOM could impact or outright prohibit generative AI models from being used for clinical decision-making, and in more restrictive states, could prohibit generative AI-related tasks even where a licensed provider supervises the AI. Developments related to the application of CPOM to generative AI in healthcare should be monitored, especially as they are expected to evolve with the proliferation of AI.

Professional Licensing

The type and nature of services supported through AI/ML technology should also be carefully considered.

Practice of Licensed Professions

AI/ML technologies could potentially constitute the practice of different types of healthcare professions, including, without limitation, medicine or psychology, which could implicate state laws regulating the scope of practice and licensure of a healthcare practitioner. Industry actors should consider, among other things, the scope of practice, licensure, and marketing laws (e.g., the white coat rule) of the states where AI/ML technology could be used.

Although some generative AI models have shown the capability to pass the United States Medical Licensing Exam, those models cannot be independently licensed to practice medicine at this time. Whether healthcare-related AI/ML products could be interpreted to be practicing or purporting to practice a profession for which a license is required should be considered. At this time, an AI/ML product should be warned against representing or holding itself out as offering services and/or including the name of a licensed profession in its product name, such as therapy or counseling, as these can be defined as licensed professions, with board or other requirements.

Informed Consent

Because unlicensed practice of a licensed profession can result in penalties for the owner and/or developer of the AI and various types of civil liability, such as tort claims and class actions, the following considerations should be carefully evaluated: (1) whether the descriptive language of the AI services could be interpreted to fall within the scope of the practice of healthcare professions; (2) whether informed consent should include additional descriptions of AI interplay or other disclaimer language for services using AI; and (3) what guardrails should be implemented to enhance transparency and patient trust. For example, if an AI-enabled software or application queries patients on their symptoms to triage them for next steps, such as whether to call a physician or go to an emergency room, and subsequently provides health advice, such actions could constitute the practice of medicine and run afoul of a state's medical licensure laws.

Professional Decision-Making and Reliance on AI/ML

Providers are likely to ultimately remain responsible for their own medical decision-making within the applicable standard of care (subject to any delegation, collaboration, or supervision requirements in the case of some providers), regardless of the tools they rely upon to inform those decisions. Where provider use of generative AI tools to assist in patient treatment and diagnosis is not prohibited, providers must not substitute the AI's determination for their own judgment or wholly rely on such determination. Prohibitions on provider use of generative AI in patient treatment under federal or state law or state medical board rules should be monitored. As explained further below, AI/ML requires human oversight and monitoring, including of AI output and calibration. Accreditation organizations, malpractice insurance, and oversight agencies are expected to inquire and scrutinize the use of AI and risk to healthcare performance and services.

Compensation and Payment

Obtaining reimbursement for products and services in healthcare is paramount to the industry, and AI/ML's role requires special considerations.

Coverage and Reimbursement

Currently, government and commercial healthcare payors do not cover or reimburse for generative AI solutions used in healthcare, outside of a number of narrow exceptions. Industry actors should be mindful of coverage updates by federal and state healthcare programs and parity laws for governmental payors, such as regulations issued by the Centers for Medicare & Medicaid Services or state Medicaid agencies, commercial insurer policies, and provider participation or network agreements. Submitting reimbursement of items or services provided by generative AI may violate payor coverage and reimbursement rules.

Fraud, Waste, and Abuse

Traditional healthcare fraud, waste, and abuse risks must continue to be considered with regard to various uses of AI/ML in healthcare, as well as non-traditional risks unique to the use of AI/ML. Federal laws, such as the False Claims Act (which prohibits the submission of false claims for reimbursement to the federal government) and state analogues, such as all-payor statutes, false claims laws, and insurance fraud laws apply to AI/ML products, including to the promotion of purportedly free products, including as mentioned above, those that may be trading data or other technical assets in exchange for AI product access.

Risks related to these laws and the use of AI/ML include, but are not limited to (1) whether the use of AI/ML may lead to, is causing, or is contributing to overutilization or inappropriate utilization of healthcare items and services, (2) whether professional services provided with the assistance of AI must be billed under a different billing code or for fewer units of time, and (3) whether AI/ML-powered

billing and reimbursement software may create inaccurate, erroneous, or up-coded claims.

For example, if a physician utilizes an AI diagnosis tool to diagnose a patient, and the tool results in the physician either not performing the same diagnostic or treatment professional services that the physician normally would perform absent the use of the AI, or spending less time to do the same, how such activity affects the preparation of a related claim, including appropriate billing codes and time units, should be considered. Another important example is determining whether the use of the same billing codes by a physician without the assistance of an AI tool in performing the same services with an AI tool would be considered up-coding.

Intellectual Property

In creating and developing AI/ML, intellectual property is a quickly evolving area and an important legal consideration. Litigation is ongoing around the unlicensed use of source material to train AI/ML. For example, artists have sued AI companies claiming that the services violate copyright and unfair competition laws. Understanding from where the data to train the model originates and, if appropriate, whether rights to use the data have been obtained is critical to the successful commercialization of an AI product.

There are also challenges to obtaining a copyright or patent for work created by AI. For example, the U.S. Copyright Office has issued guidance that requires copyright registration applicants to disclose the inclusion of AI-generated content. The U.S. Copyright Office states in its guidance that any works submitted that are entirely created by AI cannot be copyrighted, but that, on the other hand, AI-generated content with sufficient human authorship may support a copyright claim. Similarly, under recent case law, AI cannot be an inventor of a patent—only a natural person may be. This is another area that will continue to develop, and as it does, guidance from the U.S. Copyright Office or the U.S. Patent and Trademark Office should be tracked.

U.S. Food and Drug Administration (FDA)

The use or assistance of AI/ML algorithms in making clinical decisions may bring the technology within the purview of FDA regulatory authority if it meets the definition of a medical device. Medical devices are categorized into class levels with increasing levels of regulatory controls. AI/ML technologies that fall into the categories of software as a medical device and AI/ML-enabled medical devices are FDA-regulated. The FDA has released multiple guidance documents, including guidance on AI/ML-based software as a medical device, frameworks for risk categorization, quality management systems, and clinical evaluation. The research and development of AI technologies may also require informed consent or Institutional Review Board approval in certain situations involving safety and efficacy evaluations. Notable activity by the FDA in this space includes providing breakthrough device status to certain AI/ML products that address a significant public health need, such as mental health services.

The Federal Trade Commission (FTC)

The FTC oversees, and may impose limitations on, claims of AI/ML under its enforcement of consumer protection laws to prevent deceptive and unfair business practices. The FTC has released guidance on AI advertising claims, and the FTC commissioner has provided public statements reinforcing FTC's purview over potentially deceptive claims involving AI. The FTC's broad enforcement powers allow it to take actions that can be business model-breaking to AI/ML developers, including requiring the destruction of AI/ML algorithms and models that were developed in violation of law. As detailed above, deceptive practices may be based on data collection or use that is inconsistent with its terms of use, privacy policies, or representations to the public.

Medical Research and Development

AI/ML can analyze massive sets of raw data in the healthcare industry quickly and efficiently to identify patterns and make predictive conclusions. It can also assist with customized care and real-time individual or public health needs. While such analysis allows providers and researchers to avoid data overload, it is important to review the characteristics of the data itself and relevance in what it is applied to. In addition to the proceeding data privacy considerations, agency guidance, such as the FDA's discussion paper: Using AI/ML in the Development of Drug & Biological Products, should be considered, as well as the data's representativeness of the targeted population, data quality, algorithm validation, and transparency in sharing algorithms.

Careful consideration of the data can mitigate the material risk of under-representative data sets, which can magnify preexisting biases in the healthcare system, as well as reduce risks of poor generalizability of an algorithm to new settings or circumstances, the lack of alignment with informed consent, and failure to follow research protocol requirements. For example, while AI can enhance efficiency in clinical research, such as through improving patient recruitment and protocol design, algorithms may not properly account for differences in patient populations, complex protocol design, or inconsistent language in eligibility criteria.

The use of AI in research and development can be significant to IP rights and competitive markets. Failure to obtain the appropriate consents or licensure to data used for research or development can impact IP rights to the underlying AI product or service. Disclosing confidential information or relying on AI output for development can undermine the ability to obtain or retain exclusive rights to products or services.

Ethical Considerations of AI Use in Healthcare

AI/ML has the potential to both improve and exacerbate concerns of health inequity, especially as caused by the social determinants of health (SDOH). The incorporation of SDOH into AI/ML technologies may provide higher quality of care. However, human monitoring and oversight is a key mechanism to promote ethical deployment of AI and to monitor AI's potential harms. The possibility of AI/ML inflicting harm in healthcare encompasses a broad range of malicious and unintended consequences, including to the tremendous detriment of whole societies, such as biohacking and the creation and use of bioweapons.

Bias and Discrimination

While the utilization and development of AI implicates a variety of ethical concerns, these issues are exacerbated and extrapolated within the healthcare industry. Ethical frameworks have been developed by a variety of stakeholders, including the AMA, WHO, and academia. Ethical risks of AI in healthcare include that the source and integrity of data underpinning AI/ML technologies can greatly impact their accuracy and consistency and, ultimately, cause bias and discrimination. Biases can be further perpetuated in data sets as a result of the inaccuracies in data resulting from its human-annotated nature. Algorithms may incorporate biases at multiple stages of their development and can consequently compound and perpetuate preexisting inequities in the healthcare system.

Integrity of Healthcare Delivery

The risk at the forefront of using AI/ML technologies in healthcare is that these systems can sometimes be inaccurate, which could result in patient harm. Generative AI systems have been known to hallucinate and create false information. Inaccuracies can also be caused by algorithmic biases. Security is another risk that comes with the very sensitive and large data sets necessary to produce quality AI/ML models for healthcare use cases. This hallucination and false information is an example of how AI, by its very nature, can extrapolate any bias, discrimination, or misinformation quickly and extensively if it is not mitigated or caught.

Protecting against Potential Healthcare AI Liabilities

Because U.S. regulation of AI/ML in healthcare remains in flux, how to safeguard AI/ML product users against harm, as well as how to allocate responsibility, should harm occur, should be considered.

Adverse Events

Adverse events caused by AI/ML products will likely be difficult to prove and seek damages for due to the black box nature of complex AI/ML products. Where an injury or other harm has occurred, it may be difficult to prove that an AI/ML product caused such harm, as there may be little-to-no transparency or insight into how the AI/ML product operates. Appropriate and clear terms of use and performance standards should be in place to ensure liability and indemnification are provided for AI/ML product arrangements. In addition, consideration should be given to which, if any, oversight and safety mechanisms should be implemented to monitor and test the outputs of AI/ML products. Further, as mentioned above, patient education and informed consent is an important consideration to allow patient autonomy and transparency in treatment.

Oversight and Safety

Although AI/ML models and algorithms themselves are often black box systems of which the end user (and sometimes the developer) has little-to-no insight, users can put in place oversight and safety mechanisms to test and audit the outcomes of such systems. Questions such as whether certain oversight and safety mechanisms should be implemented to mitigate risk while preserving the utility of the AI/ML product should be consistently evaluated. Industry actors utilizing AI/ML products could consider extracting random output samples for review. For example, in the case of an AI/ML product that outputs diagnosis or treatment-related information, healthcare providers could create a randomly selected set of outputs to subject to peer review and auditing to confirm whether the outputs are satisfactory. Again, accreditation organizations, insurers, and oversight agencies are expected to grow scrutiny and look to risk assessments on the implementation of these products and services in healthcare operations.

Product and User Liabilities, and the Importance of Terms of Use

Product liability and medical malpractice law are two areas that bring potential liability risk for AI/ML products. Product liability can occur with design defects, manufacturing defects, and a failure to warn. Medical malpractice may arise with the healthcare provider interpreting and taking actions based upon AI/ML tools. Carefully drafting the terms of use for AI/ML is critical to properly assign risk between the developer of the AI/ML tool and the healthcare provider. As with informed consent documentation, whether appropriate terms of use are in place, along with the terms of use themselves, should be evaluated to ensure whether there are sufficient protections against all potential liabilities attributable to AI/ML and developer.

While the federal and state governments have yet to directly regulate AI/ML product liability, European countries are already promulgating AI product liability policies. For instance, the European Commission has proposed an AI Liability Directive, which would put in place evidentiary disclosure requirements for stakeholders of high-risk AI systems, and a rebuttable presumption of a causal link between the AI system and the alleged harm. Although these rules are not currently applicable in the United States, the evolution of these European policies should be monitored, as federal and state governments may look to these policies as models for domestic policies.

Conclusion – Successful AI Requires Sophisticated Regulation and Regulatory Counsel

The healthcare regulatory framework surrounding AI/ML is unsettled and still developing, yet there are far-reaching implications. Unless the federal government adopts wide-ranging, preemptive rules for the creation and use of AI/ML products, the rise of a patchwork of varying state laws, with overreaching global standards, is likely to govern this arena. As a result, legal developments require careful monitoring, and industry actors should proceed with caution and thoughtful citizenship when developing AI/ML products or entering into arrangements to use AI/ML products. It is key to build flexibility into AI/ML products and arrangements to ensure they can adjust and pivot as needed to accommodate legal developments to come.

The revolutionary nature of AI/ML catalyzes healthcare's age-old oath to care for patients and to do no harm. This oath, in using AI, must be applied in a broader and more deliberate manner to encompass the many, and society at large, to ensure that the benefits of AI in healthcare are not reaped at the cost of individual or public rights and safety.

Related Content

Resource Kits

- Clinical Trials Resource Kit
- Generative Artificial Intelligence (AI) Resource Kit
- Health Information Privacy and Security Resource Kit
- Healthcare Fraud and Abuse Compliance Resource Kit
- HIPAA Resource Kit

State Law Comparison Tool

- Healthcare Fraud and Abuse Laws Topic in the Healthcare State Law Comparison Tool
- Nonphysician Practitioners Licensing Topic in the Healthcare State Law Comparison Tool
- Physician Licensing Topic in the Healthcare State Law Comparison Tool

Practice Notes

- Corporate Practice of Medicine and Other Key Healthcare Management Contract Legal Issues
- HIPAA Privacy, Security, Breach Notification, and Other Administrative Simplification Rules
- Licensure of Healthcare Professionals
- Medicare Reimbursement
- Medicare Reimbursement Appeals
- Privacy and Confidentiality in Clinical Research

State Law Surveys

- Clinical Research State Law Survey
- Corporate Practice of Medicine State Law Survey
- Physician Licensing State Law Survey

Checklists

- Medicare Reimbursement Audit Checklist

Sara Shanti, Partner, Sheppard Mullin

Sara Helene Shanti is a partner in the Corporate Practice Group in the firm's Chicago office.

Areas of Practice

Sara's practice sits at the forefront of health-technology. Her practice focuses on providing practical counsel on healthcare innovation and complex data privacy matters. Using her medical research background and HHS experience, Sara advises providers, payors, start-ups, and technology companies, and their investors and stakeholders on digital and novel healthcare regulatory compliance matters, including artificial intelligence and machine learning (AI/ML), augmented and virtual reality (AR/VR), data assets and privacy, gamification, implantable and wearable devices, and telehealth.

Sara has deep experience advising clients on data use and protection under Part 2, HIPAA, GINA, and state privacy laws, such as BIPA and CCPA, and multinational border transmissions. She also assists clients in implementing compliance programs, launching health innovations and investments, and responding to governmental investigations. Her experience extends to consumer and patient rights, including under the American Disabilities Act and Section 1557, medical staff relationships, and navigating the evolving regulatory landscapes for next-generation technology.

At the cutting edge of advising on "data as an asset" programming, red team technology reviews, and information blocking and interoperability under the 21st Century Curse Act, Sara's practice includes mergers and acquisitions involving crucial, high-stakes, and sensitive data in areas of digital health platforms, medical and wellness devices, and web-based applications and treatment.

Sara also has deep experience with telehealth prescribing laws, including the Ryan Haight Act, and with entities offering areas of sensitive healthcare, such as behavioral health, fertility, genetics, and substance abuse.

Sara serves as an advocate for minor and patient rights, working as a court-appointed guardian. Before receiving her law degree, Sara applied her biology degree towards medical research projects, concentrating on epigenetics and immunologic responses in cancer patients. Prior to private practice, Sara worked for the U.S. Department of Health and Human Services' Office for Civil Rights.

Phil Kim, Partner, Sheppard Mullin

Phil Kim is a partner in the Corporate and Securities Practice Group in the firm's Dallas office.

Areas of Practice

Phil advises various types of healthcare providers in connection with transactional and regulatory matters. He counsels healthcare systems, hospitals, ambulatory surgery centers, physician groups (including non-profit health organizations, or NPHOs), home health providers, and other healthcare companies on the buy- and sell-side of mergers and acquisitions, joint ventures, and operational matters, which include regulatory, licensure, contractual, and administrative issues.

Phil has a particular interest in digital health. He has assisted a number of multinational technology companies entering the digital health space with various service and collaboration agreements for their wearable technology. He also assists public medical device, biotechnology, and pharmaceutical companies, as well as the investment banks that serve as underwriters involved in the public securities offerings for such healthcare companies.

Phil's client relationships are characterized by an authenticity – he communicates honestly and directly so that clients can understand issues from all perspectives and make decisions that will serve their best interests. He maintains a positive rapport with all parties to his transactions, which include:

- Healthcare arrangements and provider agreements of all types, including the transition of hundreds of physicians from a prior physician group to a new NPHO with a restructured employment model
- Professional services agreements, clinical and educational affiliation agreements, lease agreements, business associate agreements, and other services agreements between healthcare companies and various other entities in both the private and public sectors.
- Securities filings on behalf of public healthcare companies.

On the regulatory side, clients value Phil's ability to attend to details while also staying focused on the big picture. He regularly advises on healthcare compliance issues including:

- Liability exposure, the Stark law, anti-kickback statutes, and HIPAA/HITECH privacy issues
- State and federal healthcare laws
- Complex business structuring and formation issues
- Employment issues
- Matters involving various government agencies, including different state Medicaid agencies, the Texas Medical Board, and Medicare Administrative Contractors.

Christopher Rundell, Associate, Sheppard Mullin

CJ Rundell is an associate in the Corporate Practice Group in the firm's Chicago office and a member of the Healthcare Team.

Areas of Practice

CJ advises healthcare corporations on mergers and acquisitions and other corporate transactions and governance matters. His representative work experience includes representation of healthcare provider and management organizations, technology companies, commercial insurers, managed care organizations, Medicare Advantage health plans, nonprofit and for-profit health systems, academic medical centers, community hospitals, and post-acute and sub-acute providers such as home health and hospice providers, and behavioral health providers.

CJ also provides regulatory guidance to a variety of healthcare clients, such as hospitals and health systems, provider groups, technology companies, telehealth providers, and insurers on myriad regulatory matters such as HIPAA privacy and security compliance, information blocking and interoperability implementation and compliance, physician contracting, healthcare fraud and abuse compliance and investigation, corporate practice of medicine compliance, licensure and accreditation, and Medicare and Medicaid enrollment and compliance.

Previously, CJ was a healthcare transactional and regulatory associate in the Chicago office of an *AmLaw 100* law firm with a nationally-recognized healthcare practice.

Arushi Pandya, Associate, Sheppard Mullin

Arushi Pandya is an associate in the Governmental Practice in the firm's Washington, D.C. office.

Areas of Practice

Arushi advises healthcare clients on regulatory and transactional matters.

Prior to joining Sheppard Mullin, Arushi was an associate at a large Texas firm. While at Texas Law, she served as Managing Editor of the Journal of Law and Technology, Pro Bono Scholar, Dean's Fellow, Community Engagement Director of the Women's Law Caucus, and a health law research assistant. She also interned at St. Jude Children's Hospital, the American Health Law Association, and Decent, Inc. during her time in law school. Arushi received her B.S.A. in Biology and B.A. in Plan II Honors from the University of Texas at Austin.

Elfin Noce, Associate, Sheppard Mullin

Elfin Noce is an associate in the Intellectual Property Practice Group in the firm's Washington, D.C. office. He also is a member of the Privacy and Cybersecurity Team.

Areas of Practice

Elfin counsels his clients on a wide range of data privacy and cybersecurity matters.

Elfin's practice includes managing cyber breach response, drafting incident response plans, breach simulations, drafting privacy policies, negotiating and drafting complex technology agreements, and defending companies in cybersecurity litigation. His experience spans a wide range of privacy regimes, including CCPA, GDPR, telecommunications privacy (both the Cable Act and CPNI regulations), HIPAA, GLBA, TCPA, automated license plate reader regulations, and CALEA.

As in-house counsel at Charter Communications, Elfin led the company in operationalizing privacy, cybersecurity and technology matters. He advised on internal policies, breach investigation and response, drafting and negotiating privacy and data security contracts, and responding to legal requests for subscriber information.

He previously worked in-house advising a large employer health care plan with over 100,000 members on a wide range of legal issues, focusing in particular on the intricacies of HIPAA, including negotiating business associate agreements, day-to-day compliance issues, training, and notice drafting.

Elfin holds a CIPP/US certification from the International Association of Privacy Professionals.

Elfin also volunteers his time with the Washington Legal Clinic for the Homeless, assisting those in the Washington, DC area who are homeless, or at risk of becoming homeless, and in need of legal assistance.