Now & Next
Healthcare Alert

October 3, 2024

Key legal considerations at the crossroads of healthcare and technology

By Andrew Share, Jeremy Wolk, Jason Kunze, Valerie Breslin Montague, and April Schweitzer[i]

How will technology impact healthcare? Your legal team can help.

What's the impact?

- Healthcare organizations must work hand-in-hand with technology, data security specialists, and legal teams with subject matter expertise on the intersection of healthcare and technology.
- Legal counsel should assist healthcare providers with contracting for, and the use of, technology to ensure compliance with healthcare and data privacy legal and regulatory regimes.

Technology has infiltrated all aspects of our lives, including healthcare. As the healthcare industry manages its own growth from technological advancement, these innovations must be properly implemented and thoughtfully utilized. As a highly regulated industry, healthcare organizations must collaborate not only with technology and data security specialists but also with compliance and legal teams that possess subject matter expertise on the intersection of healthcare and technology.

For healthcare providers with technology infiltrating their practice, we have identified several areas where attorneys specialized in healthcare technology can provide substantial value.

Executing agreements with third-party vendors

With ever-evolving electronic medical records systems, data analytics, vital signs wearables, and medical billing systems, healthcare providers must engage numerous third-party technology vendors to both implement innovations for the most complicated healthcare functions and run the most basic administrative activities of their practices. The agreements for engaging these outside technology vendors are often filled with industry-specific jargon and complex issues regarding functionality, security, data privacy, and liability. Below are some of the categories of technology vendor agreements and key areas where legal guidance can prove helpful:

- **Information Technology:** Information Technology (IT) is a broad term that refers to the systems and devices used to access, store, retrieve, process, and transfer information. IT service providers often package services, such as IT maintenance, system monitoring, data backup, web development and design, and more together. Critical areas in IT agreements include project definitions, technical specifications, delivery milestones, data access rights, cybersecurity obligations, service levels, and self-help mechanisms.
- **Supply Chain:** A supply chain is the logistics system through which materials, commodities, and services are sourced for a company to provide its finished product and services to its end users. There are numerous participants in supply chains, including suppliers, manufacturers, distributors, retailers, wholesalers, and customers. Given the complexity of the parties and activities involved, it is imperative that supply chain agreements skillfully address the key areas of planning, sourcing, production, distribution, and returns. Also, as recent history has reminded us (whether due to Covid-related shutdowns, Suez Canal congestion, or sourcing shortages), attention to standard "boilerplate" provisions, such as force majeure clauses, can be crucial in addressing supply chain challenges.
- **Website and Apps:** An online presence via a website or mobile application and the commonization of telehealth have become crucial for healthcare providers to attract, inform, and communicate with patients. Whether these platforms are used for educational purposes, resource sharing, connecting patients and providers, or maintaining protected health information (PHI), most healthcare providers engage external parties for such services. This introduces yet another layer of legal considerations involving regulatory and contractual matters, including legal enforceability, patient privacy, and data collection, sharing, and storage .
- **Cloud-Based Services:** Cloud-based services are application and infrastructure resources that exist on the Internet rather than on hardware or software. Many of the most common software packages used in the healthcare industry are distributed as cloud-based services

external to the healthcare provider's information systems. Legal considerations with vendor agreements for these services require careful attention to warranties, cybersecurity protections, data breach processes and notifications, limitations of liability, indemnities, and regulatory compliance.

Drafting and analyzing terms for websites, apps, and wearables

Modern healthcare providers use technology to enhance their offerings and make their services and findings more accessible. Based on the type of information exchanged, it is imperative that the terms and conditions and privacy statements on a healthcare provider's website or app properly inform users how their information is protected, used, and disclosed. Below are the two most common types of agreements used with these technologies, but healthcare providers should also consider when such terms are superseded by the generic terms used by primary domain providers and application distribution platforms (e.g., Apple App Store, Google Play):

- **Terms and Conditions:** Terms and conditions—also referred to as "terms of use" or "terms of service"—refer to the duties and rights of parties hosting or visiting a website. Similarly, a mobile application or other licensed software will use an end-user license agreement (EULA) to communicate license conditions to users. This information is meant to provide users with expectations of the services offered and may create or limit specific rights between hosts and visitors for legal purposes. Terms and conditions often include permitted and prohibited activities related to privacy and data security. These terms and conditions can be critical for ensuring a user's privacy, securing data, and protecting providers from liability.
- **Privacy Policies:** A privacy policy provides users with information about the data being collected, how it is stored and used, who the data is shared with, and their rights regarding the data. Although there are no federal laws requiring a website or platform to provide a privacy policy (except under the Children's Online Privacy Protection Rule (COPPA) if directed to children under 13 years old), a detailed privacy policy may insulate a business from potential legal issues arising from disputes over data-handling practices. Furthermore, a privacy policy can build trust with users by being transparent about data-handling practices.

Data collection, machine learning, and artificial intelligence (AI)

In the modern world, healthcare data is collected and analyzed to improve patient outcomes, reduce costs, and guide decision-making processes. The collection of large data sets, the use of machine learning, large language models (LLMs), and other AI tools can provide opportunities for data analyses but also come with privacy and data security challenges. It is important that

healthcare providers understand the types of technologies used internally and externally by vendors to avoid running afoul of regulatory requirements and contractually address relevant risks. Examples of technologies used to collect data include:

- **Web Scraping:** Web scraping or data scraping—using automated tools to extract large volumes of information from the internet—can be used to quickly assemble large amounts of data. However, the details of how the scraping is performed can greatly affect risk.
- **Artificial Intelligence:** Artificial intelligence is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. See 15 U.S.C. § 9401. Healthcare providers must ensure that users of their platforms know how their data may be used for training AI models and where data is stored for analytic purposes. Additionally, federal and state agencies are developing and adopting regulations regarding the use of AI in healthcare systems.

Protecting and monetizing intellectual property

Intellectual Property (IP) refers to intangible creations of the mind and is a cornerstone of all technological advancements. Issues related to IP may arise when managing the ideas, inventions, and works of authorship of doctors, employees, contractors, and consultants. The following are the main types of IP recognized in the United States:

- **Patents:** Patents are government-granted monopolies to build, sell, and use an invention while preventing others from doing so. In the healthcare industry, medical devices and tools are typically patented.
- **Trademarks:** Trademarks are words, phrases, symbols, or designs that identify and distinguish a good or service. Healthcare providers and vendors utilize trademarks to build their brands and protect their reputations from competitors seeking to take advantage of unsuspecting customers.
- **Copyrights:** The legal right to copy and authorize others to reproduce their own work for owners of an original product. Copyrights may be used by healthcare providers who actively do research and write papers or create presentations for conferences. Additionally, copyright can protect against unauthorized copying of healthcare software and databases.
- **Trade Secrets:** Information a business has made significant efforts to keep confidential due to some value received. Within healthcare, trade secrets may include patient lists, contract terms, key customer information, and pricing information.

Software in healthcare

Software is used throughout the healthcare industry for a variety of purposes. Software used in maintaining electronic health records (EHR) of patients—also referred to as electronic patient record software (EPR) or electronic medical record software (EMR)—is an example of widespread adoption that has occurred over the last decade. Additionally, software may leverage medical databases of diseases, symptoms, and treatment plans to support medical research, diagnosis, and imaging. Software is also increasingly used to manage insurance coding and billing for medical procedures.

Most healthcare providers have also implemented software for electronic prescribing, telemedicine, appointment scheduling, and billing. Larger health systems also often use management software to assist with the day-to-day administration of equipment and inventory, including tracking and ensuring proper supply and maintenance. Moreover, wearable technology often uses software to collect patient information sent through servers to healthcare providers or back to users in digestible data.

Beyond the various examples of healthcare software, healthcare providers may face questions regarding open-source software. This software is distributed with its source code, making it available for use, modification, and distribution, subject to an applicable open-source license. In some instances, open-source software can present significant security vulnerabilities, while others require improvements developed by a healthcare provider to be freely distributed to other users of the software. Healthcare providers also may consider developing, acquiring, or licensing software assets.

It is prudent for a healthcare provider to have each of the scenarios above closely evaluated by legal counsel to ensure compliance with the legal and regulatory regimes governing the healthcare provider and achievement of the business purposes for use of such software.

The importance of experienced healthcare technology counsel

Healthcare providers can ensure that their medical practice and services are maintained at the highest standards through the use of technology. When implementing a new modality or using technology in a new manner, healthcare providers must consider and proactively address the myriad of inherent regulatory, business, and liability issues. Nixon Peabody's attorneys have extensive healthcare and technology industry experience that can be leveraged to answer your questions, educate your team, prepare compliant policies and procedures, and draft and negotiate agreements to navigate compliance, mitigate risk, and avoid liability.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Andrew L. Share
603.628.4053
ashare@nixonpeabody.com

Jason T. Kunze
312.425.3973
jkunze@nixonpeabody.com

April E. Schweitzer
312.977.4365
aeschweitzer@nixonpeabody.com

Jeremy J. Wolk
585.263.1050
jwolk@nixonpeabody.com

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

---

[i] Philip Cramer, a legal intern in Nixon Peabody's Healthcare practice and a 2026 J.D. candidate at Loyola University Chicago School of Law, assisted with the preparation of this alert.