The Evolving Landscape of Complex Litigation

Case Management, Technology, and Security

By Kathrin Hashemi

This article expands on current issues in litigation and provides practical tools that can be implemented into litigation strategies, ranging from quick solutions to more robust options.

Pharmaceutical and medical device companies have observed many shifts in the litigation climate over recent decades. Extraordinary medical advancements have been coupled with complex mass tort litigation, which has become more challenging to control. There is a critical need for the defense bar and in-house counsel to adapt to evolving litigation practices. Those who employ strategic case management solutions, utilize technology when appropriate, and apply cybersecurity measures will be able to better serve their stakeholders. This article expands on current issues in litigation and provides practical tools that can be implemented into litigation strategies, ranging from quick solutions to more robust options.

How Did We Get Here? The Industry's Evolution

Significant scientific and technological advancements have transformed the industry. Emerging research techniques have led to the discovery and development of new drugs, therapeutics, implants, prosthetics, biopharmaceuticals, and gene therapies. And since the completion of the Human Genome Project in 2003, such advancements have contributed to a deeper understanding of how genetics can influence disease susceptibility and response to treatment. The remarkable progress in scientific advancement has been accompanied by massive efforts to implement more technology into the field, resulting in significant breakthroughs, but also raising questions about new methodologies.

In addition to incorporating technology into research and development, innovations have allowed for technology to be used to increase information-sharing, provide more comprehensive data analysis, and improve patient monitoring systems. As an example, the widespread adoption of electronic health records (EHRs) and the digitalization of medical records has transformed healthcare practices, allowing for more efficient management and use of patient information by physicians and other medical personnel. Alongside these improvements, there have been extensive shifts in health care regulations and compliance. These changes have required pharmaceutical and medical device companies, as well as those in the medical field, to adapt to an environment where they are now stewards for personal health information and bear responsibility for any misuse of that information.

While technology has provided patients with better care and outcomes, the general population has also gained greater access to information about developments in the industry, as well as risks and benefits of treatment options. Patients are easily able to search for information on the Internet or connect with the rising number of consumer advocacy and watchdog groups. In addition, the COVID-19 pandemic heightened public awareness and interest in the medical arena. Overall, this result has a number of implications for drug and medical device litigation. As the general public becomes more knowledgeable, there is a growing demand for accountability from pharmaceutical and medical device companies. In addition, there has been an increased level of scrutiny and an expectation of safety and effectiveness of drug and medical device products. A

Kathrin Hashemi is a director at KCIC, a Washington, D.C.-based litigation-tech consulting firm that helps companies manage their liabilities. A DRI corporate member and a frequent attendee of DRI Seminars, KCIC works with corporations that are defendants in mass tort litigation in the manufacturing, chemicals, and pharmaceuticals industries. Kathrin has nearly a decade of risk management and consulting experience with a background in project management, technology optimization, and litigation solutions.

study conducted by IMS Consulting & Expert Services measuring safety levels of jury-eligible respondents found that 83% agreed that medical devices and pharmaceuticals should be accompanied by warnings about every potential risk or side effect, no matter how remote or tangential. Jill M. Leibold, PhD and Nick Polavin, PhD, The Rise of Safety-ism Is Influencing Verdicts, Expert Services (May 2023), ***https://www.expertservices.com/insight/safetyism-influencing-verdicts***.

Further impacts to litigation include the increased frequency and value of "nuclear" jury verdicts (i.e., those that exceed $10 million). Changing jury demographics and sentiments (as mentioned above), social inflation trends, and third-party funding have all contributed in part to rising verdicts. These massive verdicts pose a critical challenge to businesses, law firms, and the insurance industry – driving up economic burdens and the cost of future cases. In review of almost 1,400 nuclear verdicts from 2010 to 2019, an analysis found that almost a quarter of the verdicts were comprised of product liability cases (involving prescription drugs, medical devices, automobiles, herbicides, talcum powder, tobacco, and asbestos claims). Pennsylvania and Illinois were highlighted in the study due to the fact that they had some of the highest cumulative nuclear verdicts. In these jurisdictions, pelvic mesh manufacturers saw verdict awards as high as $120 million, and testosterone-boosting drug bellwethers received an initial verdict of $150 million. Cary Silverman and Christopher E. Appel, Nuclear Verdicts Trends, Causes, and Solutions, U.S. Chamber of Commerce Institute for Legal Reform (September 2022). It is no coincidence that these two jurisdictions have also been flagged by the American Tort Reform (ATR) Foundation's *Judicial Hellholes* report. This report is published on an annual basis and highlights venues that are deemed to employ unfair legal systems and are challenging for defendants in civil litigation. American Tort Reform Foundation (ATRF), Judicial Hellholes (December 2022).

Another aspect influencing change in drug and medical device litigation is the regulatory environment. As the oldest comprehensive consumer protection government agency, the Food and Drug Administration (FDA) has always been responsible for the regulation of drugs, but only was afforded regulatory rights for medical devices in 1976 through amendments made to the Federal Food, Drug, and Cosmetic Act (FDCA). As scientific knowledge has advanced, new regulations have been put into place and guidance documents have been issued to provide clarity and recommendations on various products under its purview. As an example, in recent years, the FDA has implemented stricter product labeling and warning requirements for both drugs and medical devices through amendments to the Code of Federal Regulations (CFR), Title 21. These amendments have expanded product labeling requirements, notably with respect to identification of specific risks and warnings. Moreover, in the past several years, the FDA has undertaken re-review of medical devices in sharper detail. Products such as breast implants, hip implants, and nitinol-containing devices have been the subject of particular scrutiny, triggering re-evaluation of these products and additional post-market studies.

A review of the Federal Judicial Caseload Statistics as of March 31, 2022, reveals over 630,000 civil cases remain pending in U.S. district courts. More than 80,000 of these cases pertain to pharmaceutical and medical device litigation and are situated in Multi-District Litigations (MDLs) across the country. Federal Judicial Caseload Statistics 2022, U.S. Courts (2022), *https://www.uscourts.gov/statistics-reports/federal-judicial-caseload-statistics-2022*.

Given the substantial volume of litigation and the continuous impact of scientific and technological advancements, it is essential that defendants and their counsel implement strategies that address the significant challenges faced in handling cases within the pharmaceutical and medical device industries.

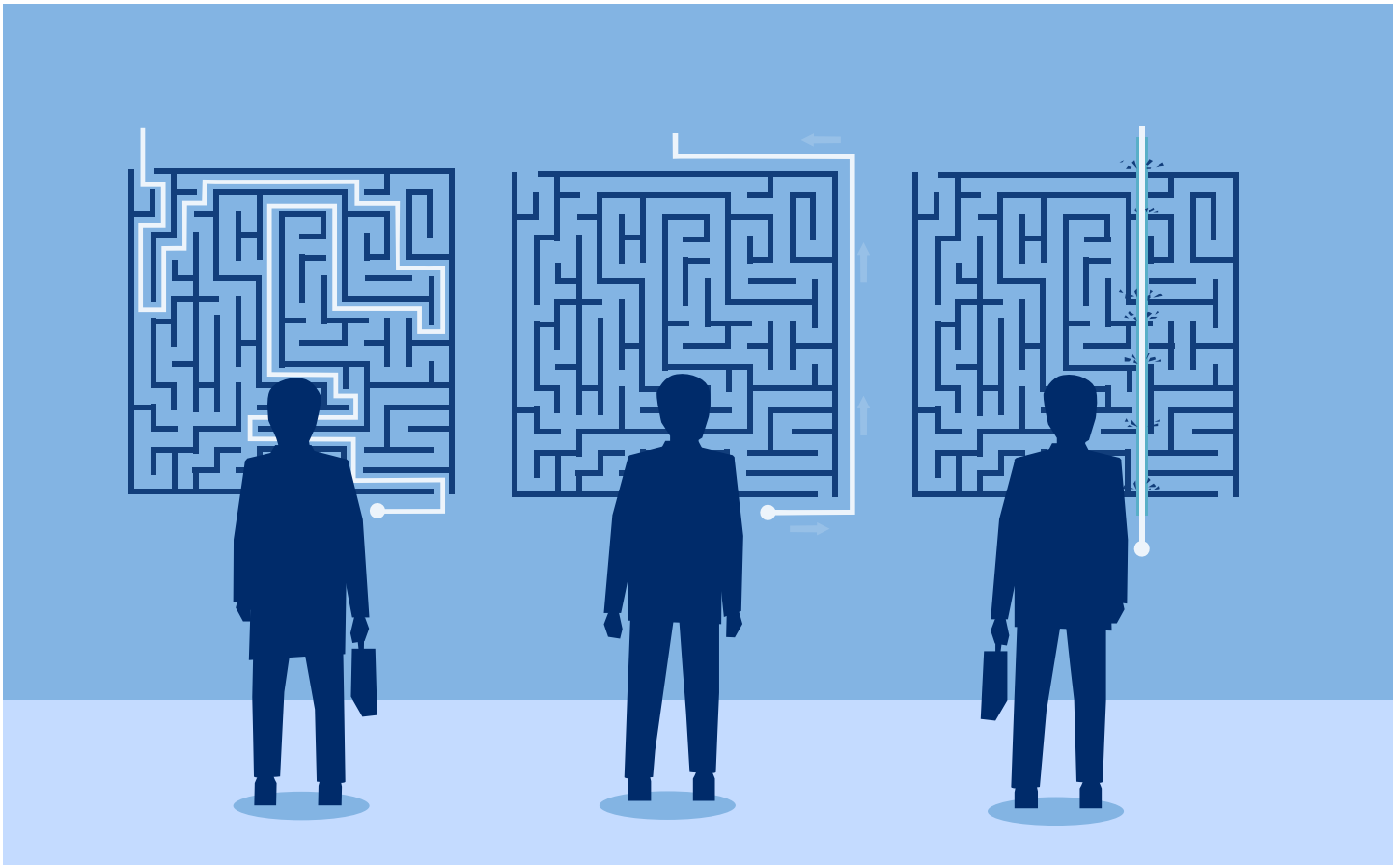
Defense Strategies and Risk Management

There is no standard or "one size fits all" approach when it comes to identifying litigation management solutions for defendants, their counsel, and relevant stakeholders. There are a multitude of considerations. For example, it is essential to consider contrasting litigation management needs between small-to-medium sized businesses (SMBs) and larger multi-national corporations (MNCs), which often have varying resources available. As important, defendants need to take into consideration the risk threshold of their business, and those of their investors, if applicable. Evaluating the availability of insurance coverage, the nature of the products involved, and public perception of the brand/corporation are all critical as well. By thoroughly assessing these factors, defendants can strategically develop a litigation management plan that safeguards their interests and promotes efficient and cost-effective case resolution. Potential solution combinations should, at a minimum, include the following components: case management, technology, and security.

Case Management: It All Begins with Data

A case management system is an integral component of any litigation management plan. There are a variety of different options available and, depending on the company, one may be better suited than another. However, the foundation for any system is data: stored in an organized, consistent, and timely manner. Litigation data points are often initially tracked in physical documents, emails, or basic spreadsheets. These methods may fit a defendant with a very small caseload; however, they do not offer the infrastructure required if information needs to be summarized quickly or if voluminous dockets develop. Another key component of a litigation management plan is to implement the system as early as possible. Oftentimes in complex litigation, defendants will need access to historical information for reporting, which can be expensive to reconcile retroactively. It can be helpful for defendants to consult with data experts to devise a solution that aligns with current requirements, but also one that can scale over time.

It is possible for an initial case management data model to utilize a spreadsheet; however, it should track critical information about the cases. At a minimum, it should include plaintiff, jurisdiction and court information, identification of defense



and plaintiff counsel, filing and service dates, product usage and maintenance details if applicable (including dosage or implantation dates), prior medical history, and adverse event reports. These data should be tracked in a standardized manner within the spreadsheet. If there are multiple individuals responsible for collecting and entering this information, standard operating procedures should be created to track the uniform manner in which data should be entered. In addition, the spreadsheet should utilize technology that allows for multiple individuals to collaborate within the file at one time, and should employ versioning control/backups. The spreadsheet should also have data validation constraints built into the file to aid with quality control measures. Defendants may also want to track multiple case types within a spreadsheet to allow internal risk managers and in-house counsel to have a full picture of the overall litigation risk the defendant is facing. In these instances, it is important to have a classification for each case (e.g., product liability, qui tam).

While this methodology of tracking case data may work for a defendant with fewer cases, more robust options may be needed. For example, a MNC with more litigation would likely need a system that has more infrastructure and higher-grade technology. Various firms offer case management platforms that utilize database technology, can be accessed online, and are customizable. While similar data points would need to be tracked, as discussed above, such comprehensive systems offer the capability to track more information in a standardized manner, including other defendants named in the case, medical histories, resolution information, tenders, related parties, and critical documents. Detailed and unique information can also be stored in metadata fields, allowing for customized fields when necessary. In addition, these systems also can streamline integral processes, offer reporting, and automate the dissemination of information in a timely manner. For example, new cases can be automatically assigned out to counsel using designated assignment rules, algorithms can sift through case information to quickly identify high-risk cases, interactive reports can show trends segmented out by a variety of parameters, and automated emails can send key updates to stakeholders on a periodic schedule. These systems also offer stakeholders direct access to data and documents. Users can be granted select permissions to view, upload, edit, and delete documents and data. Therefore, parties can be provided access to subsets of cases, if desired. Case management systems also typically offer the added benefit of either receiving feeds of data or having an internal analyst team input the information into the database (e.g., from court-ordered Plaintiff Fact Sheets (PFS)).

When evaluating a case management platform, it is always important to consider what controls exist behind the scenes to ensure that useful data is being stored in the system. After all, reporting and analytics are only as good as the quality of the data that is input into the system. Case management platforms with data validation protocols are the gold standard of these systems. Data validation protocols

use a combination of logic checks and other guidance to maintain data integrity. For example, these checks can automatically scan for instances where a date of birth was entered into the system, but the date fell after the date of death. Irregular data patterns such as this are flagged for users, who are then guided to correct the discrepancy. Sound data generates valuable insights.

Robust systems such as these are incredibly powerful tools for defendants, as they can streamline the housing and utilization of various types of information. Oftentimes, the information tracked extends beyond case information. For example, a defendant entangled in complex litigation often must look back to insurance coverage to assess how much coverage is available. Sifting through insurance coverage can be a time-intensive endeavor, but if policies are tracked in a systematic method, it can be done efficiently. Defendants need to track when self-insured retentions (SIRs) are exhausted and policies are triggered at the appropriate time. Having access to organized spend data can allow for quick reports to be generated to demonstrate proof of underlying exhaustion. Hosting spend data within the same system can allow for the generation of specialized analytics to show trends, such as defense cost by jurisdiction or by case type. These trends can then be used to better allocate resources or understand the relationship between defense costs and settlement resolutions.

The reality of current litigation is that data is now being leveraged to help formulate the basis for strategic decisions, both on the individual case level and for global/national defense plans. It allows stakeholders to address the most fundamental questions such as: How many cases and plaintiffs do we have? Who are the main parties/firms filing lawsuits? What have our resolution patterns been with a certain firm or case type over the past five years? How much are we spending on defense and settlement of cases? How much is this litigation going to cost us over the next several years? The answers to these key questions can then be utilized in discussions among risk managers, attorneys, the C-suite, investors, and other stakeholders.

Technology: Making Sense of the Data

Maintaining good data is an important step to developing a litigation management plan; however, it is essential that the data can be used to expedite decision-making and improve outcomes. With standardized data, one is able to easily report, summarize, and group the information into useful, actionable information. Many new and exciting technologies are now on the market that can be leveraged to propel litigation strategies. Some of the more important technologies include visualizations, dashboards, Artificial Intelligence (AI), and system collaborations.

One of the key technologies available is PowerBI, a business intelligence tool that offers summarizing visuals using dashboards. There are several different types of data visualization services available in addition to PowerBI, such as Tableau and Sisense. Such tools allow litigation teams to customize key charts and visualizations that suit their routine reporting needs, as well as identify unique trends or outliers that may need addressing. These reports have the ability to display vast ranges of data (historical and current) and can be interactive, allowing users to implement filters to drill into specifics. For example, interacting with the reports can limit them to a specific time range, analyze case patterns in a certain jurisdiction, or evaluate resolution trends from a particular firm. Reports can focus on a variety of subject matters including case filing trends, high-risk case attributes, or depict insurance coverage availability and erosion. These reporting models are also very flexible, and can be updated as reporting requirements evolve over time. Dynamic reporting such as this can be transformational for litigation management.

One of the most integral components of this reporting functionality is the live feed connection to the database. Therefore, when an update is made to a case, that information is passed through to the dashboard reports. Typically, new data can be incorporated into the dashboards on a periodic basis (e.g., hourly or daily). This ensures that information is up to date, but not changing as one is working in it. Access to current data allows for critical decisions to be made with the best information available.

Live, interactive reporting such as this continues to evolve over time. One of the most frequently discussed topics in litigation currently is the use of AI systems within discovery processes, research, drafting and other legal proceedings. While there is much to be learned about these systems, it is important to first recognize that all AI systems are not equal. AI is a field that has been around since the 1950s, and there are a multitude of definitions circling the ether. However, for the purpose of this overview, we will utilize Cornell University's definition: "Artificial intelligence or AI is the use of machine learning technology, software, automation, and algorithms (the automated computational application of rules) to perform tasks, [and] to make rules and/or predictions based on existing datasets and instructions." Artificial Intelligence (AI), Cornell Law School (May 2023), ***https://www.law.cornell.edu/wex/artificial_intelligence_(ai)***. Furthermore, there are several categorizations of AI, but the key concerns surround generative AI, which is a pre-trained model that seeks to formulate unique outputs based on learned information. In recent months, several courts have issued orders requiring attorneys to disclose any use of AI in the preparation of filings of any kind with the court.

While there are many concerns regarding generative AI, notably including potential biases, errors, and overall trustworthiness, non-generative AI has been continually used in many different applications. For example, visualization and dashboard reports can use algorithmic AI modeling to generate reports for reserving and forecasting. Since the models can be set up to pull in extensive amounts of data, they can plot historical trends and map out estimates of projected trends. This allows for high-level projections to be derived much more quickly, allowing individuals to focus on the rationale behind the figures.

Another technological advancement that has improved efficiencies for the litigation community has been the ability to connect multiple systems. For example, while a legal team may have a need to utilize several different systems (e.g., eBilling, case

management, and document discovery), the systems can collaborate with each other and share data. Current technology allows for systems to send feeds of data from one to another, allowing information to stay up-to-date, even across multiple platforms. By allowing information to flow seamlessly between systems, it allows for an efficient and streamlined workflow. In addition, this information then can be used in the primary system (typically the case management system) for reporting purposes in dashboards and other analytics.

Security: It's When, Not If

As security breaches become more prevalent and publicized, companies are now focusing on digital and cybersecurity plans as a strategic business priority. Many say that it's not if, but when, a company will experience a security-related event. Law firms in particular are often considered high-risk targets of cybersecurity events due to the sensitive, privileged and valuable information they handle. Law firms store and handle highly confidential client information, including financial records, intellectual property, trade secrets, litigation strategies, and personally identifiable information (PII). This makes firms obvious targets for cybercriminals seeking to exploit or monetize such information.

Law firms can take several proactive steps to protect sensitive data and help reduce the likelihood of a security threat. While these steps are suggestions, it is essential that companies and their counsel self-assess their risks and devise plans that best protect them.

Implement Strong Security Measures: Firms should establish robust cybersecurity measures, including firewalls, encryption, antivirus software, intrusion detection systems, and secure remote access protocols. Access to sensitive information should be limited based on job roles and responsibilities to ensure that data and documents are only available to the necessary individuals who require it. Further, law firms should utilize a secure data storage system (e.g., cloud storage, virtual data rooms, secure document management systems, or client portals). Any information transmitted through communication channels should be encrypted to protect contents. For example, documents should not be attached to emails. If possible, they should be shared through a secure file-sharing system, or encrypted at a minimum.

Employee Education and Training: All firm personnel should be educated on best practices by conducting regular training sessions and providing ongoing awareness campaigns to reinforce safe technology habits. According to Verizon's 2023 Data Breach Investigations Report, compromised credentials are responsible for 61% of all cybersecurity breaches. 2023 Data Breach Investigations Report (DBIR), Verizon (2023). Frequent trainings to educate employees can help them know how to properly handle their credentials, use strong passwords, identify phishing emails, and avoid suspicious websites.

Data Protection Compliance: Firms should ensure they remain apprised about applicable data protection regulations and ensure compliance with requirements, such as HIPAA, the General Data Protection Regulation (GDPR), and any local jurisdiction-specific requirements (e.g., California Consumer Privacy Act (CCPA)).

Incident Response Plan: While it may be unpleasant to plan for contingencies, it is essential that firms develop a comprehensive incident response plan. This plan should outline the steps to be taken in the event of a cybersecurity incident. There should be clear roles and responsibilities, communication protocols, as well as procedures for containment, investigation, and recovery.

Risk Management & Third Parties: Firms should consider investing in cyber-insurance coverage if they have not already, as it can help mitigate financial losses in the event of a cybersecurity incident or data breach. In addition, companies, their counsel, and other stakeholders should all be mindful of the security practices implemented by those with whom they collaborate (each other and other parties). In data management, it is essential that each party involved does its part in protecting information and maintaining security within their networks (not just its own network, but the networks with which it interacts). In partnering with a new company, firms should also ensure that the new company adheres to adequate security standards and practices. Another component of risk management involves industry standards and compliance certifications. Whenever possible, companies should strive to obtain these credentials, as they help demonstrate credibility in this area (e.g., International Organization for Standardization (ISO) compliance audits, Privacy Shield certification, and System and Organization Controls (SOC) audits).

Historically, ensuring the safety of critical firm information and documents primarily involved physical security measures. However, contemporary strategies now require a multi-layered approach that extends beyond traditional means. Neglecting legal and regulatory requirements for data storage, retention, and privacy can expose organizations to substantial legal risks, financial penalties, and damage to their reputation. Taking the necessary steps to safeguard information can be a laborious task, but when the time comes for protocols to be activated, the value will be evident.

The medical community has witnessed remarkable advancements over the past few decades; however, these advancements have brought about increased litigation and coordination efforts by the plaintiffs' bar. The rise in cases, larger verdicts, and escalating costs necessitate that defendants adopt more efficient and informed approaches to litigation management, requiring timely access to reliable information to support their decision-making processes. Implementing the technology solutions evidenced by advanced data analytics, case management platforms, and cybersecurity protocols will help mitigate the new challenges faced in drug and medical device litigation. Defendants, litigators, and other relevant stakeholders should evaluate these recommendations and determine what will help them strengthen their position in litigation.