International
Comparative
Legal Guides

Practical cross-border insights into digital health law

Digital Health

2023

Fourth Edition

Contributing Editor:
Roger Kuan
Norton Rose Fulbright

ICLG.com

Introductory Chapter

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

Digital Edition Chapter

Predicting Risk and Examining the Intersection of Traditional Principles of Product Liability Laws with Digital Health


Eric Alexander


Gerard Stegmaier


Jamie Lanphear


Michael Rubayo

Reed Smith LLP

Introduction

There is a somewhat old saw in product liability law that "law lags science; it does not lead it."[1] In the rapidly changing field of digital health, including the increasing use of software in a wide range of medical devices, law definitely lags science. While the United States Food and Drug Administration ("FDA") has issued a range of guidance documents intended to help fit digital health and software within the larger regulatory scheme for medical devices, technological advances, including artificial intelligence ("AI"), are setting a brutal pace – with product liability law changing at a comparatively glacial pace. The resulting gap is creating an exponential increase in technical, legal, and regulatory debt – some of which will most likely end up rooted in novel product liability concerns.

At its core, product liability law applies to *products* and software has generally been considered a service or intangible, not a product.[2] One consequence has been that companies that develop and sell software to the public, or companies that use software in a product that is sold to the public, have managed their possible liability for injuries or loss primarily through contractual provisions. Software is typically licensed (rarely sold) and under particular terms that include limit or cap liability, disclaim most, if not all, warranties, prevent third party beneficiaries, and contain aggressive *force majeure* provisions in efforts that have mostly shielded software developers from liability arising out of or relating to the performance (or non-performance) of their code.

Further, software is increasingly distributed and licensed in a form that does not represent its final version and often the purveyors expressly disclaim that they are not selling software at all but rather providing access to a "service." Software is often updated and changed during its lifecycle and the ability to license and distribute non-finalised programming allows for software developers to take on "technical debt." Technical debt refers to a practice of prioritising delivery of a software program or feature as quickly as possible instead of as perfectly as possible.[3] When developing software for digital health companies or for use in or as a medical device, the technical debt may compound into regulatory or legal risks as the relationship between product liability law and the law of software licensing and development, as practised, seem increasingly at odds with software being recently recognised as a product by more than one court, including in connection with electronic health records software.

Because of the significance of these issues, we seek to explain the basics of product liability law, FDA's regulation of medical devices, and recent legal developments in the context of traditional software development and risk allocation. We aim to aid software developers in digital health and those that advise them in anticipating, preparing for, and responding to this potentially rapidly changing liability landscape.

Digital Health: FDA Regulation of Medical Devices Including Software

Software has been used in medical devices since at least the 1960s. Devices containing both hardware and software components, such as MRI systems, required FDA to review not only the hardware components of the device, but also its software. In 1989, FDA issued its first draft policy on how it planned to regulate computer-based or software-based devices. As the use of computer and software devices grew and the types of devices became more complex, however, FDA determined that the draft policy had become obsolete and withdrew it in 2005. Since then, FDA has issued several guidance documents to aid manufacturers in the design, development, marketing, and servicing of safe and effective software devices.

The current framework for determining whether and how software used for medical purposes is considered a medical device, subject to FDA regulation, is complex. The Food Drug and Cosmetic Act ("FDCA") defines a device as "an instrument, apparatus, implement, machine, contrivance, implant, *in vitro* reagent, or other similar or related article, including any component, part, or accessory" intended to prevent, diagnose, mitigate, treat, or cure a disease without achieving its intended purpose through chemical action.[4] This definition excludes drugs and biologic agents, such as vaccines, but includes a full range of products, from a simple tongue depressor to AI-based devices used to alert providers of a potential stroke in patients. In 2016, Congress amended the definition of device to exclude certain types of software, including those intended to display, store, transfer, or convert formats of medical device data and results. Software intended to maintain or encourage a healthy lifestyle that are unrelated to the prevention, diagnosis, mitigation, treatment, and cure of a disease or condition are also excluded.[5]

FDA has provided details about the types of software that meet the definition of device.[6] Generally speaking, FDA considers software intended to diagnose, prevent, mitigate, treat, or cure a disease, or one intended to affect the structure of the human body, as meeting the definition of device.[7] Examples include software that can detect and diagnose a stroke in patients by analysing MRI images and software that can process images to aid in the detection of breast cancer. Certain medical mobile applications, such as apps designed to measure a patient's glucose level, are also classified as medical devices subject to FDA regulation. It is important to note that when determining whether software or a mobile app meets the definition of device, the focus is

on the software's function, not its platform. Software intended to interpret EKG waveforms to detect heart function irregularities, for example, meets the definition of device, regardless of whether it runs on an EKG machine or mobile app.[8]

Despite the fundamental differences between hardware devices and software devices, FDA has not instituted a specific approach for regulating software devices outside of its normal review process based on their risk classification. Class I devices, such as software that solely displays readings from a continuous glucose monitor, are considered low-risk and are subject to the lowest degree of regulation. Class II devices are those of moderate risk, and may include software that analyses medical images, such as mammograms. Most Class II devices require FDA clearance of a 510(k) premarket submission before they can be marketed. Alternatively, for novel medical devices that are low-to-moderate risk, manufacturers may submit a *De Novo* request for FDA to classify its device as Class I or Class II. Class III devices, such as an implantable defibrillator, pose the greatest risk to patients and are subject to the greatest degree of regulatory oversight. Such devices must obtain premarket approval ("PMA") from FDA before they can be marketed. For all classes of devices, FDA's review process focuses on safety and efficacy. FDA does not evaluate premarket submissions with an eye toward issues related to privacy and security, unless those considerations pose a potential risk to patient safety.

With the increased risk of cyber vulnerabilities inherent in software devices, cybersecurity has become a critical focus of FDA. FDA's concerns about cybersecurity relate to the impact cybersecurity threats pose to device functionality and patient safety, not privacy. FDA expects device manufacturers to identify cybersecurity vulnerabilities that increase the potential risk of patient harm and put mitigations in place, such as limiting unauthorised access to device software and using design approaches that will maintain the device's functionality, even after its security has been breached.[9] Manufacturers are expected to manage cybersecurity risks throughout the device's lifecycle by, for example, issuing regular software updates and patches and reporting to FDA any suspected cyber attack that impacted the device's performance. Information concerning how a manufacturer has addressed cybersecurity risks and how it intends to monitor and manage those risks throughout a device's lifecycle is a critical component of a PMA and 510(k) for medical device software.[10]

As healthcare continues to become more digital, the prevalence of devices reliant on software continues to grow. Modern-day devices are increasingly connected and rely on data analysis from many sources and over time to perform their functions. Ranging from smart watches tracking your steps, heart rate, and oxygen levels, to insulin pumps automatically managing an individual's blood sugar levels, devices use software to collect and use data. However, as demonstrated in recent guidance regarding Device Software Functions and Mobile Medical Applications, FDA has been careful to not imply that *all* software utilised for medical purposes satisfies the definition of device or will be subject to its regulatory authority. Some of the software functions FDA has announced it considers to be a device, subject to its regulatory authority, include:

- functions that control or analyse data from the device;[11]
- functions that transform a mobile platform into a regulated medical device by using attachments, display screens, or sensors;[12] and
- functions that perform patient-specific analysis and provide specific outputs or directives for use in the diagnosis, treatment, mitigation, cure, or prevention of a disease or condition.[13]

FDA's recent guidance illustrates the role software increasingly plays in digital health and determinations regarding whether a medical product meets the definition of device and/or is subject to FDA regulation. The guidance does not demonstrate a specific concern by FDA to protect personal data collected, analysed, and stored by the software, but rather to ensure no physical harm will be done to patients because of software malfunctions.[14] This is demonstrated by the lack of regulation for software focused only on recording or tracking health information, providing access to patient health information, or transferring health information from one healthcare professional to another, among other functions.

Product Liability

Historically

Devices

Traditional United States ("U.S.") product liability law, including as it applies to medical devices, can be hard to reconcile with existing legal models for software licensing and emerging AI and machine learning developments. First of all, unlike in the European Union or other parts of the world, there is no single source of U.S. authority that can be consulted to determine the law. Each state has its own law on product liability. Some have fairly comprehensive Product Liability Acts, but most have law shaped by the decisions of mostly state appellate courts that address the issues before them. Federal court decisions predicting state law consistent with *Erie Railroad Co. v. Tompkins*,[15] may be persuasive or they may be rejected by a subsequent state appellate court decision or legislative act. There may be issues addressed definitively by most states, but not at all by others. The resulting patchwork makes it difficult to characterise what "the law" is on a number of product liability issues. Even the Restatements of Torts have limited authority, do not address all product liability issues, and are updated infrequently.

Generally speaking, subject to variability in the defences available because of the regulatory status of the device and state law at issue, product liability for medical devices has largely resembled product liability law for other products. Liability for medical devices is most often predicated on an inadequacy in the disclosure of the device's risks, an issue with the device's design that makes it unduly risky, or a deviation from specifications in the manufacture of the particular device used by or implanted in the plaintiff.[16] A warnings claim requires proof that an adequate warning would have changed the outcome in the case, as by making the prescribing physician choose a different device that would not have produced the same outcome. A design claim often requires proof that the design was unreasonable in comparison to the alternative designs and knowledge at the time and that a device with an adequate design (i.e., without the alleged design defect) would have avoided the plaintiff's injuries. A manufacturing claim requires proof that the particular device caused harm to the plaintiff because it deviated from how it was supposed to be when it left the manufacturer's control. Each of these liability theories requires proof that the device caused the plaintiff's injuries and alleged damages. These theories do not make a manufacturer an insurer of all harms caused by its products, but require some showing of unreasonable conduct by the manufacturer or unreasonable risks attendant to the design of its product.

Three of the most significant issues determining the potential liability for a medical device manufacturer are whether the device requires a prescription, the device's regulatory status, and whether the applicable state law imposes duties beyond those

described above. The first issue is typically referred to as the "learned intermediary doctrine," which means that the duty of the manufacturer of a prescription device or other medical product runs to the physician who prescribes it, not the patient or general public. There is widespread near-national acceptance of the learned intermediary doctrine for prescription medical devices. This makes sense not just because prescription medical devices cannot be obtained legally without a prescription, but because FDA requires specific physician-facing labeling for prescription medical devices. Moreover, a manufacturer would rarely have a practical ability to ensure that any patient-facing labeling was seen by a patient before the prescription/implant/use of the device.

As discussed above, FDA's risk-classification system divides devices into three classes based on FDA's assessment of risk. This system not only affects the required route to market, but the availability of preemption pursuant to the Supremacy Clause in the U.S. Constitution. The Medical Device Amendments of 1976 ("MDA") include an express provision for preemption of state law claims that are "different from, or in addition to" a federal requirement that relates "to the safety or effectiveness" of a medical device.[17] Since the U.S. Supreme Court decision in *Riegel v. Medtronic, Inc.*,[18] most warnings and design claims against FDA-approved Class III devices are preempted and thus not viable.[19] This is not the case with regard to Class I or Class II devices, which have more limited preemption defences available. *Medtronic, Inc. v. Lohr*,[20] focused on the regulatory requirements of a device cleared before the Safe Medical Device Act of 1990, but has had a lasting impact on preemption for a wider range of Class II devices. Implied preemption under *Buckman Co. v. Plaintiffs Legal Committee*,[21] for claims predicated on violating FDA requirements, applies across classes of devices; however, treatment varies greatly from case to case. Even without preemption, evidence that a device was compliant with the terms of its market authorisation and that the manufacturer complied with all of its obligations can be powerful evidence.

Because of the power of express preemption for Class III devices, some judges have created new duties to impose liability on device manufacturers that are not "different from or in addition to" the requirements imposed by FDA approval. The path is narrow for these purported "parallel claims" because of the interplay with *Buckman's* requirement that liability not be predicated on a violation of a federal requirement. The result is that some courts have found that what might otherwise seem are purely federal requirements, like reporting adverse events to FDA, are also independent requirements of state law. There is wide variation between and within states on the endorsement of novel parallel claims to impose liability on manufacturers.

Some issues relevant to liability for software have less state variability. In general, consistent with the requirement that the product was not changed after leaving a manufacturer's control to impose liability on the manufacturer, product liability generally does not apply to another entity that merely distributed or re-sold the product.[22] In terms of a prescription medical device, the company that designed, manufactured, and sold the device into commerce may be liable under the theories discussed above, but the hospital that purchased it and charged a patient for its use will not be, absent an alteration of the device. Similarly, entities involved with the design or manufacture of the device before it leaves the manufacturer's control, like the manufacturer of a component, will not be liable under product liability principles.

Additionally, courts rarely allow an inference of a "malfunction" to suffice. It may be easy to assume that any medical complication in the anatomic vicinity of a device is due to some device failure. The concept of *res ipsa loquitur* allows a similar inference of negligence in circumstances where the defendant has sole control of the alleged instrument of injury and the injury/accident would not be expected otherwise, such as, where a sponge is found in the abdomen after a surgery, it can inferred that a negligent act or omission by the surgeon or staff in the operating suite left it there. For product liability claims regarding a medical device, however, a doctor's or patient's use of the device is not within the manufacturer's sole control and the injuries at issue are typically not something that occur only when the device fails. As such, a "malfunction" is not assumed even when some injury follows the use of a medical device.

Moreover, while the consideration of causation in medical device product liability cases can be involved, the plaintiff must typically connect a tangible physical injury to the device to recover any damages, including for mental anguish or economic loss. Asymptomatic injuries, fear of a possible injury, or the need for medical screening or possible future medical intervention are typically not compensable. Similarly, care occasioned by the recall of a device because of a potential risk of injury typically will not give rise to liability absent the device actually causing that injury in the plaintiff.

With this background in mind, there are a number of areas where the application of traditional U.S. product liability principles could differ with patient-facing digital health and software-driven medical devices. This is particularly so because software is often updated over time as weaknesses or issues become known or areas for potential improvement are identified. In today's wireless world, the ability to issue software updates and patches is largely expected[23] and whether and how affirmative consent and additional licensing provisions may apply represent on-going issues for many software developers.

The role of updates for patient-facing software-driven medical devices greatly complicates the product liability and risk-prevention analysis. For instance, a defect in design or manufacture is typically measured at the time that the product left the manufacturer's control. If a manufacturer can update software post-sale on its own, then has the product ever left its control? Does the design of a software-driven product become defective at the point updates become available to address a safety issue, but the updates are not made to the plaintiff's particular product for one reason or another? In most states, the duty to warn of risks is also measured as of the time of the sale of the product, with a minority of states recognising a post-sale duty to warn under special circumstances. This makes sense for prescription medical devices, like most products. The manufacturer can provide warnings with its device, but will typically have no mechanism to warn the prescribing physician, subsequent health care providers, and/or the patient (whose identity will almost always be unknown to the manufacturer) of subsequently attained information relevant to the device's risks. Again, this works differently with digital health and software-driven devices, where the relationship with the end-user may often continue post-sale and the ability to update software may go hand-in-hand with the ability to notify an end-user of a post-sale issue. While these issues are not unique to digital health applications of software, the consequences may be more severe and the responsibility for "users" to patch and update the software, therefore, may be much more legally complicated. Moreover, even though devices may only be available by prescription, the learned intermediary doctrine may not apply in some cases where the level of direct and/or continuing interaction between the manufacturer and patient undercuts the rationale for the doctrine. When the doctrine does not apply, the duty to warn runs to the plaintiff/patient directly, which increases the risk of product liability exposure.

Preemption of design or warnings claims involving Class III medical devices could also operate differently for software-driven

devices. For express preemption under the MDA to apply, the plaintiff's theory of liability must be "different than or in addition to" the federal requirements imposed in connection with PMA approval. In the case of a device with software that will be updated over time or where the device utilises AI or machine learning, some courts may doubt that the device at the time of the alleged injury was the same as what FDA had approved. In an arguably analogous situation, the off-label use of FDA-approved Class III devices has generally not defeated preemption of design and warnings claims that would otherwise exist.[24]

Given that product liability law has generally not applied to software, any imposition of product liability would entail making new state law. The dynamic described above in terms of purported parallel claims for Class III medical devices would likely apply with devices utilising software, machine learning, or AI. As noted above, most states do not impose post-sale duties to warn and, when they do, require there to be new information on the risk of the product, so any liability for when and how post-sale software updates are rolled out would require significant expansion. Similarly, detailed requirements for PMA are unlikely to have true parallels in duties imposed by state tort law.

Lawsuits over injuries allegedly due to a failure of software in a medical device might also name entities that contracted with the device manufacturer to develop or update that software. A parallel may be seen in the history of suing manufacturers of raw materials and component parts used in connection with the manufacture of breast implants and other implantable devices. This led to the enactment of the federal Biomaterials Access Assurance Act of 1998, as it was considered to be a matter of "national interest" to protect suppliers of raw materials and components against litigation[25] "to safeguard the availability of a wide variety of lifesaving and life-enhancing medical devices."[26] Should large-scale litigation commence against entities that design or maintain software used in medical devices, similar logic could be used to support federal limitations on liability.

Depending on whether software used in a medical device can be adjusted or personalised by the user or prescribing healthcare provider, the malfunction theory of liability could have more traction than with other devices. If software fails to perform as expected and there is no ability for it to be altered by anyone other than the manufacturer or its agents, then criteria for application of malfunction or *res ipsa loquitur* could apply. Given most software developers routinely seek to disclaim that their software can or will function, including for any particular purpose, this risk should be of keen interest to developers and their advisers.

The typical requirement of a tangible physical injury could also be loosened in product liability litigation over software or software-driven medical devices. Even setting aside potential liability for alleged privacy, which does not require physical injury, the nature of many possible software issues with devices could increase the propensity for claims of liability for fear of injury or increased risk of injury. For example, a false reading on a device that monitors heart rhythm or blood sugar could cause a patient to be concerned about the risk of a particular health outcome or to seek medical care because of the misperception of risk. Other software-related glitches with medical devices could lead to subclinical alterations in medication administration or cardiac stimulation. A software issue across a number of devices at the same time could give rise to a class action asserting product liability claims even without tangible physical injuries in the putative class members.

Software

The Restatement (Third) of Torts defines product as "tangible personal property."[27] Courts across the country have consistently found that software does not qualify as tangible property because it is typically produced for a specific purpose to satisfy the terms of a contract, or is mass produced and licensed out to each user to utilise for their designated purpose.[28] Consequently, courts typically treat software companies differently than device manufacturers by limiting their liability to contract-based theories.[29]

Software-related user licence agreements are intended by their providers to limit and manage risk, including to limit liability. It remains mostly settled law that checking a box or clicking a button or similar affirmative action can demonstrate assent to an agreement, provided the layout and language used is conspicuous and provides reasonable notice of such assent.[30] Incorporation of documentation and acknowledgment of receipt and warnings with software are increasingly commonplace and many software developers take great pains to limit their liability by contract. While courts use "shrink wrap" and "click wrap" terminology routinely in determining the existence of software-related contracts, the touchstone remains whether there is an offer, acceptance, consideration, and legality. Each of these elements is increasingly being contested in litigation and by regulators such as the Federal Trade Commission.

The concept of software liability being governed primarily by contract law is a routine fixture of liability allocation for software developers. Plaintiffs seldom recover on tort claims, with courts tending to conclude that the developer's liability begins and ends with the licence. *Murray v. ILG Techs., LLC*, demonstrates how contract law, not tort law, represents the primary theory used to recover software-related damages.[31] In *Murray*, the plaintiffs alleged damages arising from a bar-exam grading software that erroneously failed a portion of students. The district court dismissed the plaintiffs' product liability claim summarily but allowed the contract claim to proceed.[32]

Product liability trends

The issue of potential product liability for software has been the subject of discussion for some time. As set out above, in 1998, while defining a "product" for purposes of strict product liability as a tangible thing, the discussion accompanying the Restatement (Third) of Torts suggested that software, at least mass-marketed rather than *ad hoc* software, might be considered a product. This speculation was based on shaky ground, as the Ninth Circuit case it cited actually "declin[ed] to expand products liability law to embrace the ideas and expression" found in a book.[33] Over the next two decades, the treatment of software in product liability law did not change much.[34] "Courts have yet to extend products liability theories to bad software, computer viruses, or websites with inadequate security or defective design."[35] The few contrary rulings did not establish a trend, except perhaps in Louisiana. Starting with a ruling from the Louisiana Supreme Court that computer software was "corporeal property" for purposes of taxation,[36] two federal courts later found software to be a product under the unusual "corporeal moveable" definition in the Louisiana Product Liability Act.[37] In addition, an intermediate appellate court in California ruled in 2014 that the company that supplied publishing software to a pharmacy could possibly be subject to product liability for an incomplete drug monograph.[38]

In the last few years, however, the frequency of rulings on this issue has increased and it may be just a matter of time until software is subject to product liability. In *Rodgers v. Christie*,[39] the Third Circuit considered the question in a fairly unusual case of a homicide being blamed on an issue with AI software that ran the New Jersey Public Safety Assessment ("PSA") system used in connection with pretrial services for criminal matters. It held

that the PSA software "is neither 'tangible personal property' nor remotely 'analogous to' it" to qualify as a product under the New Jersey Product Liability Act.[40] In addition to "information, guidance, ideas, and recommendations" not being defined as products under the Restatement (Third) of Torts, "extending strict liability to the distribution of ideas would raise serious First Amendment concerns."[41]

Because of the defences available under the Michigan Product Liability Act, the defendant in *Holbrook v. Prodomax Automation Ltd.*[42] sought to have its software used in connection with an assembly line robot treated as a product. The broad statutory definitions allowed for the conclusion that it was a "component" of a product and thus subject to product liability. The court concluded that the "programming is an 'integral' and 'essential' part of the [assembly] line because... 'without ... the PLC program ... the robotic components would not have been orchestrated to move at all within the line.'"[43] However, the court did limit its ruling to software as a component of a product, noting that the "programming need not qualify as a product itself."[44] By contrast, the conclusion that "programming was completed at the facility does not make it any less a part of the product's design," suggests that some expected downstream modifications may not affect product liability for software as a component of a product.[45]

Because of the quirks in Michigan law, the *Holbrook* decision, like the Louisiana decisions before it, did not signal a sea change in the treatment of software as a product for purposes of tort liability. Indeed, after the *Holbrook* decision, a federal court in Washington issued two orders finding that an online video game was not covered by the state's product liability statute.[46] The game was "software as a service, not an 'object,' hence Plaintiff's product liability claim must fail as a matter of law."[47] Additionally, recent litigation over automobile accidents allegedly caused by distracted driving due to use of software applications on mobile devices has not yet produced direct decisions on whether social media applications/platforms are "products" for purposes of strict liability, because the plaintiffs in those cases have pursued negligence-based theories.[48]

In late 2022, the Fourth Circuit issued its decision in *Lowe v. Cerner Corp.,*[49] which is the first decision that has found software to be a product that is likely to have precedential value outside of one state. At the district court level, the developer and seller of an electronic health records system was granted summary judgment on product liability claims related to injuries to a patient during post-surgery in-patient care, largely because the hospital had made changes to the system after purchasing it.[50] This was so despite the system being "designed to be easily configured by the customer." On appeal, the Fourth Circuit reversed, holding that the plaintiff had presented sufficient admissible evidence of a design defect, a failure to warn, and proximate causation to get to trial on product liability claims against the software developer. However, nowhere in the district court decision, the Fourth Circuit decision, or a vigorous dissent in the Fourth Circuit was there a direct ruling on whether the electronic health records system was a product. That may be because Virginia does not recognise strict product liability. Instead, all recognised product liability claims sound in negligence.[51] Still, a federal circuit decision that takes for granted that an electronic records system – an adaptable software package – is a product subject to the core product liability claims of design defect and failure to warn should not be minimised when projecting the future of digital health law.

The elephant in the room on the role of product liability in allegations of harm from software is the recent creation of a Multidistrict Litigation proceeding in *In re: Social Media Adolescent Addiction/Personal Injury Products Liability Litigation*, pending in the Northern District of California. By its name, this is "products liability litigation" that focuses on parents' allegations that their minor children suffered various harms due to a number of social media platforms. The U.S. Judicial Panel on Multidistrict Litigation characterised the common allegations against the social media platforms being "defective because they are designed to maximize user screen time, which can encourage addictive behavior in adolescents."[52] Because of the nature of Multidistrict Litigation, claims implicating the laws of almost all of the states will be the subject of extensive litigation.[53] This makes it highly likely that the issue of whether strict product liability applies to social media platforms, including the software that runs them, will be decided directly. Those decisions, potentially modified on appellate review, will inevitably influence the legal playing field for potential claims relating to digital health and software-driven medical devices.

New practices of software companies who are manufacturers/sellers

As discussed above, software-development lifecycle best practices are likely to evolve further and familiarity with FDA's risk classification schemes may be a useful starting point for many developers, regardless of whether their software is or may be a medical device. Not only is it possible that companies that develop software for use in or as a medical device will be subject to specific additional requirements, but those that provide software that may be used in digital health or as components in digital health products may find it desirable to take specific additional steps to manage the uncertainty of emerging risks in this area. Greater disclosures regarding the software, specific testing and quality enhancements and improvements, very deliberate approaches to patching and update responsibility and support, and other thoughtful solutions may be helpful to software developers and those who support them. It seems likely that standard-setting bodies and efforts, and additional prescriptive regulations may also come into play. Not only has FDA noted that its authority in this area is limited and should be revisited,[54] but the agency's reluctance to over-classify software used in devices as a "device" and the role of standards is already getting some attention.[55] At the same time, in announcing its National Cybersecurity Strategy March 1, 2023, the Biden Administration stated that because "[s]oftware makers are able to leverage their market position to fully disclaim liability by contract" creating disincentives to use "secure-by-design principles or perform pre-release testing" the U.S. must "begin to shift liability onto those entities to take reasonable precautions."[56] Whether this policy will carry over into digital health and medical devices specifically remains to be seen.[57] In any event, medical device companies, software developers who work with them, and those who assist each with managing and responding to liability risks will benefit from greater understanding of and monitoring this emerging area of the law.

Endnotes

1. *Rosen v. Ciba-Geigy Corp.*, 78 F.3d 316, 319 (7th Cir. 1996) (Posner, J.).
2. "A product is tangible personal property distributed commercially for use or consumption." Restatement (Third) of Torts: Products Liability §19(a) (1998). At the time of this statement, the discussion included the comment that "Under the [Uniform Commercial Code], software that is mass-marketed is considered a good. However, software that was developed specifically for the customer is a service." After the Uniform Commercial Code was

amended in 2005, however, it defined "software" as a "general intangible," not a "good." *Id.* §9-102(42); *see also* U.C.C. §9-102, Commentary, at 4(a); Uniform Computer & Information Technology Act of 2002 §102(a)(35) (likewise defining "information"—as opposed to "goods"—as including "computer programs").

3. *Technical Debt*, Product Plan, https://www.productplan.com/glossary/technical-debt/.
4. 21 CFR 520(h).
5. 21 CFR 520(o)(1)(B); *see also* General Wellness: Policy for Low-Risk Devices (Sept. 27, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices.
6. *See, e.g.*, Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act (Sept. 27, 2019), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act; Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications; Clinical Decision Support Software (Sept. 28, 2022), https://www.fda.gov/medical-devices/software-medical-device-samd/your-clinical-decision-support-software-it-medical-device.
7. Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), at 6, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications.
8. *Id.*
9. Content of Premarket Submissions for Management of Cybersecurity in Medical Devices (Oct. 2, 2014), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.
10. *See* Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (Apr. 8, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions.
11. *Id.* Examples include an automatic Insulin pump and digitally controlled blood pressure cuff.
12. *Id.* Examples include attaching blood-glucose strip readers or ECG electrodes, and utilising built-in functionality, such as accelerometers or other sensors, for medical purposes.
13. *Id.* Examples include a dosage calculator for radiation therapy and blood-glucose tracker for abnormal levels.
14. *Id.* at 11 ("FDA intends to apply its regulatory oversight to *only* those software functions that are medical device and whose functionality *could pose a risk to a patient's safety* if the device were to not function as intended") (emphasis added).
15. 304 U.S. 64 (1938).
16. In general, absent unusual facts of a direct relationship between a patient and medical device manufacturer, theories based on express or implied warranties or misrepresentation are unavailable or subsumed within a design or warning theory. Similarly, consumer protection statutes generally do not provide recovery for personal injuries allegedly caused by medical devices or other products.
17. 21 U.S.C. § 360(a).
18. 552 U.S. 312 (2008).
19. True manufacturing defect claims are not preempted because a requirement of approval of a Class III medical device is that what is sold should match the design that was approved and such claims are based on the absence of a match.
20. 518 U.S. 470 (1996).
21. 531 U.S. 341 (2001).
22. According to the Restatement (Third) of Torts, Products Liability §1 (1998), strict product liability "applies only to manufacturers and other commercial sellers and distributors who are engaged in the business of selling or otherwise distributing the type of product that harmed the plaintiff." Some state statutes have similar broad definitions, but the general practice in product liability lawsuits involving medical devices is that manufacturers are the targets and the entities with control over design, labeling, and manufacturing. Indemnity and contribution provisions in contracts between manufacturers and distributors/re-sellers are common and often imposed by law even in the absence of contractual provisions.
23. *See* Vincent J. Vitkowski "The Internet of Things: A New Era of Cyber Liability & Insurance," Declarations, International Association of Claim Professionals, at 3 (Spring 2015) (predicting "IoT devices comprised of integrated hardware and software systems will almost surely be treated as products").
24. *See, e.g., White v. Medtronic, Inc.*, 808 F. App'x. 290 (6th Cir. 2020); *Shuker v. Smith & Nephew, PLC*, 885 F.3d 760 (3d Cir. 2018); *Caplinger v. Medtronic, Inc.*, 784 F.3d 1335 (10th Cir. 2015).
25. 21 U.S.C. § 1601(16).
26. 21 U.S.C. § 1601(15).
27. Restatement (Third) of Torts: Products Liability §19(a) (1998).
28. *See Flores v. Uber Techs.*, No. 19STCV24988, 2022 Cal. Super. LEXIS 9648 (Cal. Super. Ct. L.A. Cnty. Mar. 22, 2022) (holding that software application is a service not a product); *Shema Kolainu-Hear Our Voices v. ProviderSoft, LLC*, 832 F. Supp. 2d 194 (E.D.N.Y. 2010) (software not subject to tort liability because of existence of a licence); *Murray v. ILG Techs., LLC*, 378 F. Supp. 3d 1227 (S.D. Ga. 2019) (granting summary judgment against software-related product liability claims).
29. One recent example is *Quinteros v. Innogames*, where a product liability claim involving an online video game was dismissed because it was "software as a service" and thus not a product. *See Quinteros v. Innogames*, No. C19-1402RSM, 2022 U.S. Dist. LEXIS 55640, at *19 (W.D. Wash. Mar. 28, 2022).
30. *See Sgouros v. TransUnion Corp.*, 817 F.3d 1029, 1033-34 (7th Cir. 2016); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229 (E.D. Pa. 2007); *Jallali v. Nat'l Bd. of Osteopathic Med. Exam'rs, Inc.*, 908 N.E.2d 1168 (Ind. Ct. App. 2009).
31. *Murray v. ILG Techs., LLC*, 378 F. Supp. 3d 1227 (S.D. Ga. 2019).
32. *Id.*
33. *See Winter v. G.P. Putnam's Sons*, 938 F.2d 1033, 1036 (9th Cir. 1991). The Reporters' Notes to Restatement (Third) of Torts §19 had cited earlier dicta in the same decision that "Computer software that fails to yield the result for which it was designed may be another" intangible treated as a product for the purposes of product liability. *Id.* at 1035.
34. *See, e.g., Sanders v. Acclaim Entertainment, Inc.*, 188 F. Supp.2d 1264, 1278-79 (D. Colo. 2002) (computer games are not

products for strict liability purposes); *Wilson v. Midway Games, Inc.*, 198 F. Supp.2d 167, 173 (D. Conn. 2002) (interactive "virtual reality technology" is not a "[product] for the purposes of strict products liability"); *James v. Meow Media, Inc.*, 90 F. Supp.2d 798, 810 (W.D. Ky. 2000) ("While computer source codes and programs are construed as 'tangible property' for tax purposes and as 'goods' for UCC purposes, these classifications do not indicate that intangible thoughts, ideas, and messages contained in computer video games, movies, or internet materials should be treated as products for purposes of strict liability."), *aff'd*, 300 F.3d 683, 700–01 (6th Cir. 2002) (software makers and website operators do not deal in "products").

35. James A. Henderson, Tort vs. Technology: Accommodating Disruptive Innovation, 47 Ariz. St. L.J. 1145, 1165 n.135 (Winter 2015) (citation and quotation marks omitted). *See also* Seldon J. Childers, Don't Stop the Music: No Strict Products Liability for Embedded Software, 19 U. Fla. J.L. & Pub. Pol'y 125, 151–52 (2008) ("The weight of authority, including case law, finds software is not defined as a 'product' for purposes of tort products liability.").
36. *South Central Bell Telephone Co. v. Barthelemy*, 643 So.2d 1240, 1244 (La. 1994) ("[W]e hold that computer software at issue in this case constitutes corporeal property under our civilian concept of that term.").
37. *Corley v. Stryker Corp.*, No. 6:13-CV-02571, 2014 WL 3375596, at *1, 4 (Mag. W.D. La. May 27, 2014), (applying strict liability under the LPLA to the software in a medical device "designed and manufactured from patient-specific 3D imaging data ... and the use of proprietary 3D imaging software[]" because it was "a necessary part" of the "product"), *adopted*, 2014 WL 3125990 (W.D. La. July 3, 2014); *Schafer v. State Farm Fire & Casualty Co.*, 507 F. Supp.2d 587, 600–01 (E.D. La. 2007) (based on *South Central Bell*, a computer "program may be a product for the purposes of the LPLA").
38. *Hardin v. PDX, Inc.,* 173 Cal. Rptr.3d 397, 407 (Cal. App. 2014) ("But [plaintiff's] theory is that [defendant's] software program, not the information it produces, is the defective product ... [To survive the state court equivalent of a motion to dismiss] causes of action need only be shown to have minimal merit.").
39. 795 F. Appx. 878, 880 (3d Cir. 2020).
40. *Id.*
41. *Id.*
42. No. 1:17-cv-219, 2021 U.S. Dist. LEXIS 178325 (W.D. Mich. Sept. 20, 2021).
43. *Id.* at *16–17 (internal citations omitted).
44. *Id.* at *17.
45. *Id.* at *18.
46. *Quinteros v. InnoGames*, No. C19-1402RSM, 2022 WL 898560 (W.D. Wash. Mar. 28, 2022); *Quinteros v. InnoGames,* No. C19-1402RSM, 2022 WL 953507, at *2 (W.D. Wash. Mar. 30, 2022) ("The Court will not consider new argument related to Plaintiff's product liability claim" and "[i]n any event, Plaintiff has failed to demonstrate manifest error").
47. *Id.* at *7.
48. *Lemmon v. Snap, Inc.*, 995 F.3d 1085, 1092–93 (9th Cir. 2021) (plaintiff asserted negligent design theory, but referred to a social media application as a "product"); *Maynard v. Snapchat, Inc.*, 870 S.E.2d 739, 746 (Ga. 2022) (plaintiffs "pursued only a negligence theory of design defect" and also repeatedly referred to the same application as a "product"). *Cf. Grossman v. Rockaway Township*, No. MRS-L-1173-18, 2019 WL 2649153, at *15 (N.J. Super. Law Div. June 10, 2019) (dismissing on other grounds but finding "no facts alleged that would support the theory that [the social media site's] actions qualify or constitute a product under the [New Jersey] Product Liability Act"). Decisions thus far in other litigation over social media have also not directly addressed the viability of product liability allegations. *See Doe v. Twitter, Inc.*, 555 F. Supp.3d 889, 929–30 (N.D. Cal. Aug. 19, 2021) (not reaching question of whether social media is a product; dismissing action for other reasons); *Williams v. Apple, Inc.*, No. 4:19-cv-00782, 2020 WL 1296843, at *2–4 (S.D. Tex. Mar. 24, 2020) (product liability claims involving cell phone software update dismissed for multiple other reasons; status of update as a "product" not addressed); *Herrick v. Grindr, L.L.C.*, 306 F. Supp.3d 579, 592 n.9 (S.D.N.Y. 2018) ("not address[ing the website's] argument that it is not a 'product' for purposes of products liability" given dismissal for other reasons), *aff'd*, 765 F. Appx. 586 (2d Cir. 2019).
49. No. 20-2270, 2022 WL 17269066 (4th Cir. Nov. 29, 2022).
50. *Lowe v. Cerner Health Servs., Inc.*, No. 1:19cv625, 2020 WL 6829770 (E.D. Va. Nov. 20, 2020).
51. *See, e.g., Powell v. Diehl Woodworking Mach., Inc.*, 198 F. Supp. 3d 628, 633 (E.D. Va. 2016) ("Virginia law only recognizes three products liability claims: negligent assembly or manufacture, negligent design, and failure to warn.").
52. *See In re Social Media Adolescent Addiction/Personal Injury Prods. Liab. Litig.*, __ F. Supp. 3d __, 2022 WL 5409144, at *2 (J.P.M.L. Oct. 6, 2022).
53. As of February 16, 2023, there were already 132 separate actions pending in the nascent proceeding. https://www.jpml.uscourts.gov/sites/jpml/files/Pending_MDL_Dockets_By_Actions_Pending-February-16-2023.pdf.
54. *See* Policy for Device Software Functions and Mobile Medical Applications (Sept. 28, 2022), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/policy-device-software-functions-and-mobile-medical-applications. (stating the "Agency will continue to evaluate the potential impact these technologies might have on improving health care, reducing potential medical mistakes, and protecting patients").
55. One of these potential standards is the ONC Health IT Certification Program, which was recently mentioned in the FDA's recent non-binding Policy for Device Software Functions and Mobile Medical Applications. In the guidance released on September 28, 2022, they listed software functions that would not be subject to regulation which included software that complied with the ONC Program.
56. *See* National Cybersecurity Strategy (Mar. 1, 2023) https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
57. *See* 4 Highlights from Biden's Beefed Up Cybersecurity Strategy (Mar. 2, 2023) https://www.law360.com/articles/1581635/4-highlights-from-biden-s-beefed-up-cybersecurity-strategy.

Eric Alexander, a partner at Reed Smith LLP, practises in the area of product liability litigation for pharmaceutical and medical device companies. He has personally tried multiple prescription drug and device cases to verdict and assisted in trying many other prescription drug and medical device cases. Eric's practice has particularly focused on scientific, medical, and regulatory issues in product liability cases, along with novel theories of liability and defence. As such, he has closely followed developments in the digital health and medtech realm, and their intersection with product liability law. Eric is also a member of the blogging team for the award-winning Drug and Device Law blog.

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9403
Email: ealexander@reedsmith.com
URL: www.reedsmith.com

Gerard Stegmaier, CIPP/US, a partner at Reed Smith LLP, focuses his practice on corporate governance, intellectual property, and technology – especially as they relate to privacy, information security, and consumer protection. An experienced and pragmatic litigator, Gerry focuses a significant part of his practice on prelitigation and advisory services relating to business strategy for these issues and is widely recognised for his work in data strategy, AI and machine learning. He often acts as strategic counsel and outside product counsel to leading innovators and disruptive technology companies advising and defending their interests, especially to avoid and navigate crises. He has helped health information technology, data management, advertising, and consumer technology companies bring some of the most popular and impactful products and services of the 21st century to market.

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9228
Email: gstegmaier@reedsmith.com
URL: www.reedsmith.com

Jamie Lanphear, a counsel at Reed Smith LLP, focuses her practice on products liability litigation for medical device and pharmaceutical companies, with a particular focus on regulatory, scientific, and technical issues. She has extensive experience representing major manufacturers in cases involving defect, failure to warn, wrongful death, and consumer protection claims, and has served on multiple high-profile mass tort trial teams..

Reed Smith LLP
1301 K Street, N.W., Suite 1000 - East Tower
Washington, D.C., 20005
USA

Tel: +1 202 414 9217
Email: jlanphear@reedsmith.com
URL: www.reedsmith.com

Michael Rubayo, an associate at Reed Smith LLP, is a computer scientist whose legal practice includes a focus on privacy, tech and data issues.

Reed Smith LLP
599 Lexington Avenue, 22nd Floor
New York, NY, 10022
USA

Tel: +1 212 549 4707
Email: mrubayo@reedsmith.com
URL: www.reedsmith.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group