Bloomberg Law

Electronic Commerce & Law Report™



*Mobile*

# The New App Economy: Products Liability in an Increasingly Mobile World

**MOBILE APPS**

Mobile apps designed to diagnose, monitor or treat diseases could pose considerable risks to user safety in the event of a malfunction. David Ferrera and Mara O'Malley of Nutter McClennen & Fish LLP discuss the Food and Drug Administration's regulatory approach for mobile medical apps and the legal framework under which manufacturers could be exposed to liability.

By David L. Ferrera and Mara A. O'Malley

In an age where seemingly everyone is glued to their smartphone, the mobile application or ''app'' economy continues to expand at a rapid pace. Total global revenue generated by apps is predicted to reach over $100 billion by 2020, according to a *Business Insider* report. Health and wellness-related apps represent a significant portion of the app market. For example, in 2015, a GlobalWebIndex report found that approximately 15% of global internet users accessed a health or fitness app monthly.

*David L. Ferrera is a partner in Nutter's Litigation Department and chairs Nutter's Product Liability and Toxic Tort Litigation practice group. He can be reached at dferrera@nutter.com.*
*Mara A. O'Malley is an associate in Nutter's Litigation Department. She can be reached at momalley@nutter.com.*

Growth in this segment is not without risks. Apps that are specifically designed to diagnose, monitor, or treat diseases pose considerable threats to user safety should the app malfunction. Internet connectivity may create additional danger of an unauthorized user compromising an app's functionality.

To help address these concerns, the FDA recently issued two applicable Final Guidance documents, one on Medical Device Accessories and the other on Postmarket Management of Cybersecurity in Medical Devices. The surge in regulatory attention paid to mobile medical apps (''MMAs'') could incentivize plaintiffs' lawyers to turn their focus to this sector. With the increased potential for litigation, it is essential that MMA manufacturers understand the legal framework that could make them vulnerable to liability.

## 1. MMAs and the FDA

The FDA defines an MMA as a mobile app that meets the definition of a device under the Food, Drug, and Cosmetic Act (''FD&C Act'') and is intended to be used either as an accessory to a regulated medical device or to transform a mobile platform (like a phone or tablet) into a regulated medical device. Under the FD&C Act, a ''device'' is essentially any non-chemical machine or implement that is intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease.

 ISSN 1098-5190

### a. Final Guidance on Medical Device Accessories

The FDA issued its Final Guidance on Medical Device Accessories on December 30, 2016. If an MMA is to be used as an accessory—i.e., if it is intended to support, supplement, and/or augment a medical device—the Final Guidance can be a helpful tool in advising manufacturers of the extent to which they will be subject to FDA regulation. The FDA designates accessories into one of three ''classes,'' each with a corresponding set of regulatory requirements, based on the level of risk the accessory poses to users. Going forward, the FDA will assess and classify an accessory separately from a parent device, based on the accessory's intended use. This is a departure from the FDA's current practice of classifying accessories with their parent devices absent evidence that the accessory presents a distinct risk to patient safety.

Additional Takeaways:

■ Only an accessory that falls into the highest risk class (''Class III'') requires premarket FDA approval; and

■ Manufacturers of novel accessories that have no current comparative product on the market, and that are not the subject of any approved PMAs or 501(k)s, should take advantage of the FDA's *de novo* process to receive a ''risk- and regulatory control-based'' classification for the new product.

### b. Final Guidance on Postmarket Management of Cybersecurity in Medical Devices

Another guidance that may directly impact MMA manufacturers is the FDA's Final Guidance on Postmarket Management of Cybersecurity in Medical Devices. Issued on December 28, 2016, this Guidance establishes best practices relative to cybersecurity concerns. This is especially relevant to MMAs with internet connectivity, but is applicable to other medical devices as well.

Since the risk of a cybersecurity breach is impossible to eliminate completely, the FDA's focus is on ensuring that manufacturers and developers establish comprehensive risk management programs to mitigate the potential for a breach. The FDA also views cybersecurity as an issue that must be borne equally by all stakeholders in the medical device field. Thus, it strongly encourages collaborative efforts amongst manufacturers, health care providers, users, and information technology vendors to combat security breaches.

Additional Takeaways:

■ Appropriate risk management programs should identify and balance the MMA's potential exploitability with the severity of patient harm that could occur in the event of a breach;

■ Due to evolving cybersecurity risks, manufacturers should implement procedures that continually work to identify and mitigate risks; and

■ The FDA strongly encourages manufacturers to participate in an Information Sharing and Analysis Organization—sector-specific forums where companies and individuals can share pertinent and often sensitive information on a particular issue—in order to communicate cybersecurity threats and mitigation strategies, and to establish best practices for combating cyberattacks.

## 2. Potential for Liability for MMA Manufacturers

With these Final Guidance documents, the FDA has offered some clarity regarding those mobile apps that it intends to regulate as well as how it will regulate cybersecurity issues. Where a mobile app meets the definition of a ''mobile medical app,'' the FDA suggests it will be regulated like any other medical device. Thus, although courts have yet to address liability for the malfunction of an MMA, one can attempt to predict how they will rule based on the same common law framework that they currently apply to FDA-governed medical devices.

As a threshold matter, plaintiffs asserting products liability claims against MMA manufacturers must establish that an MMA constitutes a ''product.'' Courts have held that computer software may properly be considered a ''good'' for UCC purposes, and a ''product'' for products liability purposes. However, determining whether an MMA is a product could be more difficult, depending on how it functions. For example, if an MMA monitors user information and makes health recommendations based on that information, akin to a medical service provider, this could blur the line between product and service. Concluding whether an MMA is a product will require a fact-intensive analysis.

### a. Who Could Be the Target of an MMA Products Liability Action?

MMA manufacturers—defined by the FDA as anyone who ''initiates specifications, designs, labels, or creates a software system or application for a regulated medical device''—will be the most natural targets for products liability actions. Excluded from the definition of manufacturer are distributors, meaning that the FDA does not intend to regulate companies like Apple or Samsung, which simply make MMAs available through the iTunes App store or a similar platform. While the FDA's exclusion does not prohibit distributors from being named as defendants, manufacturers and developers will likely remain plaintiffs' primary targets.

### b. What Types of Claims Can Defendants Expect to See?

As with other medical devices, plaintiffs might assert claims of design or manufacturing defect as the result of a malfunctioning MMA. Although software is not manufactured in the traditional physical sense, software programmers generally follow design specifications from which they are not meant to deviate. If a programmer fails to follow the design specifications, the result is a manufacturing error. However, if one failure is deemed to be the result of a flaw in the software design itself, this claim would be based on a defective design theory.

If consumers suffer injuries caused by a breach in the MMA's cybersecurity, manufacturers can anticipate traditional claims of negligence. Plaintiffs may assert that the manufacturer failed to exercise due care in identifying and mitigating potential security risks. Design defect claims are also possible if there is reason to believe a manufacturer failed to include sufficient security protocols in the initial software design.

Depending on the extent to which the risk of certain defects was appreciable at the time the MMA was intro-

   ISSN 1098-5190

duced to the market, failure to warn claims could be common as well. Effectively communicating product warnings to consumers who download MMAs to mobile platforms could prove challenging for manufacturers. Upon purchasing and downloading mobile apps, users generally enter into licensing agreements. Users notoriously fail to read these agreements, though, and there has been extensive litigation over the effectiveness of these so-called ''click wrap'' agreements in other contexts. With respect to MMAs, manufacturers who place product warnings within such agreements may face allegations that the warning was insufficient. Manufacturers may need to focus on other methods of communicating product warnings to consumers, perhaps repeating the warning each time a consumer ''launches'' the MMA.

### c. Available Defenses

Although the FDA's pre-market approval process is onerous, manufacturers of approved MMAs can benefit from that approval in defending against product liability claims. When pre-market approval is required and obtained, the FDA's determination that the product is safe and effective may bolster a manufacturer's position that it took reasonable steps to address possible defects and that it adequately evaluated the risks to user safety. Where an MMAs falls within the FDA's purview as a medical device or regulated accessory and the manufacturer secures pre-market approval, certain state common law claims may be preempted. The Supreme Court held in *Riegel v. Medtronic, Inc.*, 552 U.S. 312 (2008) that in the case of PMA-approved medical devices, state law claims for strict liability, breach of implied warranty, and negligent design were preempted by federal law (claims for breach of express warranty and negligent manufacture were not).

## 3. The Future of Liability

Courts have yet to directly address MMAs in products liability actions, so there is still considerable uncertainty over the extent of potential distributor liability and what types of security measures manufacturers can reasonably be expected to take in the face of continually evolving threats to cybersecurity. It also remains to be seen how the federal regulatory landscape may change under the Trump administration and the resulting impact on the Final Guidance documents discussed above. President Trump campaigned on a promise of deregulation and even specifically stated that he intended to ''[r]eform the Food and Drug Administration, to put greater focus on the need of patients for new and innovative medical products.'' It remains to be seen whether there is a drastic curtailing of federal regulations in the weeks and months ahead. Developers, manufacturers and even distributors should consult with counsel to ensure that they are minimizing the potential for liability and staying abreast of pertinent regulatory changes.