Published on *The National Law Review* https://natlawreview.com

Digital Health Year in Review: 2017 Trends and Looking Ahead to 2018

Article By:

Bernadette M. Broccolo

Ryan B. Marcus

Jiayan Chen

Jennifer S. Geetter

Introduction

Throughout 2017, the health care and life science industries experienced a widespread proliferation of digital health innovation that presents challenges to traditional notions of health care delivery and payment as well as product research, development and commercialization for both long-standing and new stakeholders. At the same time, lawmakers and regulators made meaningful progress toward modernizing the existing legal framework in a way that will both adequately protect patients and consumers and support and encourage continued innovation, but their efforts have not kept pace with what has become the light speed of innovation. As a result, some obstacles, misalignment and ambiguity remain.

Privacy and Cybersecurity

Cybersecurity continues to be one of today's most material and pervasive enterprise risks, and is faced by all stakeholders who are active in the digital health ecosystem. That risk will continue to escalate with the rapid demand for and proliferation of collaborations and other initiatives to promote patient and consumer engagement through digital health mobile wellness and disease management apps that collect unstructured, identifiable health care and personal information from providers, patients, consumers and others. In this context, even a minor or inadvertent violation of the law could result in significant fines and penalties, reputational harm and loss of user trust. Management of this risk demands relentless diligence in identifying and assessing risks under applicable federal and state laws and establishing, maintaining, assessing and improving privacy and cybersecurity compliance and risk management programs that include, among other things, a thorough and well-tested cybersecurity breach or cyberattack preparedness response plan.

NIAC Report on Facilitating Sharing of Information on Cyber Threats

To help address the threat of cyberattacks, the US government is soliciting the cooperation of private companies and executives. A report by the President's National Infrastructure Advisory Council (NIAC) notes, among other things, the lack of information sharing and coordination between private parties and the government as a key reason for the inability "to move actionable information to the right people at the speed required by cyber threats." NIAC's proposals include "public-private and company-to-company information sharing of cyber threats at network speed." Key questions remain unanswered regarding the potential risks and liabilities of sharing proprietary and other confidential or sensitive information with the government, which NIAC suggests would be explored via a pilot program.

FTC Privacy and Security Enforcement

In recent years, the Federal Trade Commission (FTC) has been aggressive on the federal privacy and security scene under the broad provisions of Section 5 of the FTC Act relating to consumer fraud and deceptive practices. As the growth of "patient-as-consumer" and "consumer-generated data" has accelerated, the FTC announced its plan to refine its legal framework for protecting the privacy and security of consumer information. To launch that effort, the FTC held a workshop in late December 2017 to explore how to characterize and measure the injury that a consumer suffers when information about them is misused. Acting FTC Chairman Maureen K. Ohlhausen's agenda for the workshop focused on three main components of the "informational injury" construct that has emerged from the FTC's recent case-by-case privacy enforcement framework:

- Identify the different types of injury incurred by consumers and businesses from privacy and data security incidents.
- Determine an approach to quantitatively measure informational injuries and estimate the risk of their occurrence.
- Better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing and using information.

According to Chairman Ohlhausen, the FTC will use perspectives gained from the workshop in its development of a defined framework for enforcing informational injury within the agency's expansive Section 5 jurisdiction. Digital health innovators and other businesses whose strategies rely largely on the exchange of patient and other consumer personal information should watch closely as the FTC's privacy and security enforcement plan continues to unfold.

Data Breach Enforcement

Companies that provide mobile health (mHealth) solutions (*i.e.*, mobile applications, wearables, remote monitoring devices and other mobile technologies that facilitate health care) should note that CardioNet, a provider of remote mobile monitoring, reached a $2.5 million data breach settlement with the Office for Civil Rights (OCR) of the US Department of Health and Human Services (HHS). The settlement related to two breaches of electronic protected health information (ePHI), one involving the theft of a workforce member's laptop containing ePHI from a parked vehicle, and another as to which OCR did not provide any details. OCR alleged several failures by the company to implement appropriate security safeguards required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including having policies and procedures addressing the receipt, removal and encryption of hardware and electronic media, and conducting an accurate and thorough security risk assessment. The settlement is a reminder to digital health vendors as well as other business associates and covered entities to have reasonable and appropriate measures in place to protect the security and integrity of ePHI, and that a breach may lead to a broader investigation into

the sufficiency of a company's security program.

New York – Health Insurance Company Cybersecurity Requirements

Health insurance companies licensed under New York insurance laws will need to take steps to adhere to new cybersecurity requirements that began to come into effect on a rolling basis in August 2017. These new requirements present unique compliance challenges. First, the regulations will require insurance companies to ensure the cybersecurity of not just member information, but also any "nonpublic, business-related electronic information" if the unauthorized disclosure, access or use of that information would cause a material adverse impact to the company. Second, the regulation includes a 72-hour deadline to notify the Superintendent of the New York Department of Financial Services following the discovery of a cybersecurity event or breach. Finally, starting on or before February 15, 2018, each company operating under New York banking, insurance or financial services law must file an annual certification of compliance with the new regulations. Additional cybersecurity requirements, including multi-factor authentication and encryption, will become effective in March and September 2018.

Telephone Consumer Protection Act Enforcement

A federal privacy requirement of significance to mobile device application developers and health care providers is the Telephone Consumer Protection Act (TCPA). The TCPA regulates the use of an automatic dialer to make phone calls and the sending of certain text messages to consumers prior to obtaining consent from the individual. One persistent misconception is that the TCPA applies only to marketing phone calls or "spam" text messages, and that therefore HIPAA covered entities and business associates are exempt from the TCPA. To the contrary, the TCPA applies to many automated communications between health care providers or health plans and patients, and the "safe harbor" established by the Federal Communications Commission (FCC) for health-related text messages and phone calls is very difficult to meet. With potential statutory damages of up to $1,500 per call or text message, a single phone call or text message campaign could be very costly. As a result, TCPA compliance will remain an important focus for digital health companies in 2018.

Issuance of Long-Awaited Amendment to Federal Substance Abuse Confidentiality Regulations

The proliferation of big data and other data-sharing initiatives highlights the importance of understanding the patchwork of privacy and security requirements that may apply to any given proposal to provide wide access to large amounts of data. In that regard, stakeholders should note the issuance of the long-awaited final rule amending the federal confidentiality regulations for substance use disorder records for the first time in almost 30 years. The final rule represents an effort by the Substance Abuse and Mental Health Services Administration to reduce compliance burdens by making it easier for federally assisted substance use disorder treatment programs to exchange covered information with providers through clinically integrated networks, health information exchanges and accountable care organizations. The final rule also includes certain changes that may make it easier to conduct research, quality improvement and population health management activities, although certain regulatory obstacles remain.

Class Actions to Protect Privacy of Biometric Data

At the state level, companies that collect, use or store biometric data should be mindful of an apparent growing focus by the class action bar and state legislatures on protecting biometric data, such as fingerprints, retina or iris scans, voiceprints, or hand or facial geometry scans. Illinois

residents filed at least 32 class action lawsuits in 2017 seeking to challenge companies' collection, use or storage of biometric information under Illinois law. Although Illinois is currently the only state that allows private rights of action under its biometrics law, several other states have such laws that are enforceable by their respective state attorneys general or are considering similar laws in their respective legislatures.

Other Health Information Technology Developments

21st Century Cures Act – New HHS Infrastructure for Development of Health Information Technology Policy and Standards

In 2018, HHS is expected to implement several provisions of the 21st Century Cures Act (Cures Act) relating to health information technology. As directed by the Cures Act, the Health IT Advisory Committee (HITAC) has replaced the Health IT Policy and Standards Committees. The Cures Act tasks HITAC with recommending to the Office of the National Coordinator for Health Information Technology (ONC) policies, standards, implementation specifications and certification criteria on the implementation of health information technology infrastructure, nationally and locally, that advances the electronic access, exchange and use of health information. HITAC will hold its first meetings in January 2018. Congress hopes that ONC will be able to leverage HITAC's work to encourage the consistent implementation and use of common standards, and to take steps toward achieving national interoperability.

21st Century Cures Act – Information Blocking Prohibitions and Penalties

Under the Cures Act, Congress established new civil monetary penalties of up to $1 million per information blocking violation, including potential penalties for false attestations by health information technology vendors. ONC and the HHS Office for Inspector General (OIG) are expected to release a proposed rule in early 2018 relating to information blocking. The proposed rule is expected to clarify the definition of information blocking and provide guidance on what practices *do not* fall within the definition. OIG is already reviewing cases and is preparing to take action against prospective violators under its new authority.

OIG Meaningful Use Program Enforcement

In May 2017, OIG announced a $155 million settlement with eClinicalWorks, a vendor of certified electronic health record technology (CEHRT). OIG alleged that eClinicalWorks violated the False Claims Act because it concealed material facts from its certifying body about the capabilities of its software—facts that would have invalidated the software's status as CEHRT. As a result, according to the complaint, eligible professionals participating in the Medicare and Medicaid EHR Incentive Programs (also known as the Meaningful Use Programs) received incentive payments and avoided payment reductions under the programs when they should not have, as the electronic health records they were using did not meet the specifications for CEHRT.

In addition to increasing vendor scrutiny, OIG is pushing the Centers for Medicare and Medicaid Services (CMS) to increase its efforts to detect improper payments made to health care providers participating in the Meaningful Use Programs. CMS will face continuing pressure to step up its existing auditing efforts for the Meaningful Use Programs and Merit-Based Incentive Payment System (MIPS) in response to OIG's finding in a report released in June 2017 that there may have been more than $731 million in inappropriate meaningful use payments made to health care

providers. Vendors of CEHRT and health care providers that participate in the Meaningful Use Programs and MIPS should monitor this increased scrutiny and be ready to demonstrate their compliance so as to avoid sanctions.

Telehealth

Continued Increase in State Regulation

State regulation of telehealth reached an all-time high in 2017, with 34 states and the District of Columbia passing a total of 62 legislative bills, representing a 22 percent increase from 2016. A summary of all state-approved legislation is available here. Such significant legislative activity continues to fuel concerns that telehealth is overly regulated and that the diversity of approaches has created a daunting "patchwork quilt" of state telehealth-specific regulations.

The substance and the underlying spirit and intent of much of the 2017 legislation, however, are different than in prior years. A material portion of the legislation actually included a component of *de*regulation of telehealth. For example, Texas, the state with the strictest telehealth laws that was embroiled in a multi-year lawsuit with direct-to-consumer telehealth company Teladoc, eliminated its requirement that a face-to-face encounter take place at an "established medical site"—a site with licensed or certified health care professionals, with sufficient technology and medical equipment to allow for physical evaluation, and of sufficient size to accommodate patient privacy and presentation of the patient to the provider—prior to delivering care via telehealth, unless a very limited exception applied. This change enabled a new chapter of home-based telehealth programs in Texas and ended a very public (and expensive) lawsuit.

The continued success of professional licensure compacts, such as the interstate medical licensure compact and the enhanced nurse licensure compact, is another example of states adopting solutions to reduce barriers to telehealth, as the compacts ease professional licensure requirements for health care professionals by allowing multi-state licensure through a streamlined process. The compacts have received support from federal agencies, such as the FTC and US Department of Justice, which view them as a way to increase competition and enhance access to patient care. The federal government has taken a similar approach with the passing of the Veterans in E-Health and Telemedicine Support Act of 2017 earlier in January 2018; the legislation is designed to expand the telehealth programs of the US Department of Veterans Affairs (VA) by enabling VA-licensed health care professionals to deliver care to veterans across state lines.

The focus of state legislation in 2017 also continued to move away from regulating the delivery of care (*e.g.*, practice standards for securing informed consent and remote prescribing) and toward regulating the coverage and payment of telehealth services by private payors. Today, 34 states and the District of Columbia have a telehealth coverage parity law that requires a payor to cover a service delivered via telehealth if the payor covers such service when it is delivered in person (subject to any in-network limitations). The vast majority of states with these parity laws do not require that payors pay the same amount for telehealth services as for the same type of in-person services. Therefore, payors may pay less for the telehealth service (in some cases, as little as half as much), and many of these laws have other limitations that undercut their effectiveness by providing payors with an "out," such as subjecting coverage to compliance with a payor's existing policies. For example, Arkansas only requires coverage of a telehealth service when there is an in-person examination of the patient, which was a requirement of some state professional boards in the past that has since been retired (except in the context of remote prescribing in certain cases).

Going beyond parity laws, the coverage and payment policies of commercial and government payors continued to expand in 2017. Medicaid regulations were revised in almost 20 states to lessen the telehealth coverage requirements or expand the types of telehealth covered services.

At the federal level, the US Drug Enforcement Agency (DEA) announced plans to ease the restriction on the prescription of controlled substances via telehealth as set forth in the Ryan Haight Online Pharmacy Consumer Protection Act of 2008, which requires a telehealth provider to examine a patient in-person before prescribing a controlled substance. One change may be the implementation of the long-awaited "special registration" pathway for telehealth providers found at 12 USC § 802(54)(E). The DEA announced plans to develop and implement this telemedicine registration provision to enable practitioners to use telehealth to prescribe controlled substances without performing an in-person examination in the spring of 2018. These changes may occur as the result of the DEA's own initiative to implement a "special registration" process for telehealth prescribers, which has been announced on more than one occasion over the past few years, and/or the recent White House declaration of the opioid addiction epidemic as a national emergency. Either way, telehealth providers should continue to monitor the federal remote prescribing requirements, as their ability to prescribe controlled substances via telehealth may soon change.

Expansion in Medicare Coverage and Reimbursement

One of the biggest victories for telehealth came toward the end of 2017 with CMS's release of a final rule for the 2018 Medicare Physician Fee Schedule. CMS added new telehealth codes covering health risk assessments, psychotherapy, chronic care management and interactive complexity, and expressed its commitment to "transforming access to Medicare telehealth services by paying for more services and making it easier for providers to bill for these services." CMS's recognition that improving access to telehealth services will modernize Medicare payments to promote patient-centered innovations will lead to further investment in telehealth's potential by the private payor community.

In addition, the Senate's unanimous passage of the Creating High-Quality Results and Outcomes Necessary to Improve Chronic (CHRONIC) Care Act of 2017 (S.870) in the fall was an encouraging step toward modernizing telehealth access and reimbursement, as the bill aims to improve health outcomes for Medicare beneficiaries living with chronic conditions and includes key provisions expanding access to telehealth. While many in the telehealth industry had high hopes for the passing of the House CHRONIC Care Act (HR 4579), the lack of progress and Republican support for the House bill has led commentators to question its future.

Telehealth providers should continue monitoring the ongoing changes in state laws and regulations addressing the coverage and payment of telehealth services, and the practice standards that apply to the delivery of care via telehealth.

HHS OIG Work Plan – Audits of Claims for Telehealth Services

The OIG 2018 Work Plan provided that Medicare Part B payments for telehealth services for claims where no corresponding claim was submitted by the originating site (which indicates that the originating site might not have met Medicare's telehealth coverage requirements) will be the focus of a planned audit. Medicaid payments for telehealth services were recently added to the audit to ensure compliance with Medicaid reimbursement requirements.

This increased risk of audit is a reminder to telehealth companies that they are subject to the same

compliance standards as other types of health care providers. Therefore, they need to develop, implement and monitor compliance with corporate compliance programs that reflect the Compliance Program Guidance (Essential Elements) adopted by the OIG for various types of health care entities. The Essential Elements offer valuable guidance to telehealth companies on how to create a robust and effective voluntary compliance program, including performing internal monitoring and auditing, implementing compliance and practice standards, designating a compliance officer or contact, conducting appropriate training and education, responding appropriately to detected offenses and developing open lines of communication.

Repeal of Net Neutrality

As 2017 came to a close, the telehealth industry turned its attention to a new challenge: the potential consequences of the FCC's move to repeal the Open Internet Order, which restricted internet service providers (ISPs) from interfering with the capabilities of content providers to disseminate their content utilizing the internet, and its replacement with the Restoring Internet Freedom Order. The Open Internet Order (1) prohibited blocking access to websites, throttling (or slowing down) website download speeds and requiring payment for prioritization of internet traffic, and (2) required public disclosure regarding network management practices, performance and commercial terms of broadband access services sufficient for consumers to make informed choices regarding use of such services and for content, application, service and device providers to develop, market and maintain offerings.

While the net neutrality rules were in place, the connectivity of each of these services and devices could not be restricted by the ISP operating the broadband networking to which they connected. For example, one telehealth provider could not pay to have faster connectivity speeds than another telehealth provider. Now, ISPs could (within the confines of the antitrust and trade laws) create tiered pricing structures that favor certain content providers over others. This structure could raise the barrier to entry for new health care technologies and new telehealth companies, causing rural providers or hospitals with less favorable revenues to cut innovative programs to increase access. The FCC's expressed motivation for removing restrictions on ISPs is to fuel the telehealth industry by facilitating greater investment in infrastructure, including that within rural communities, and thereby increase the ability of rural communities to gain access to high-speed internet connections. Additionally, the FCC promised that, by deregulating, ISPs will innovate and compete, providing improved options for consumers. What these new options may look like in terms of digital health tools, however, remains to be seen.

If the repeal of the net neutrality regulations creates additional costs for telehealth providers, it will be more important than ever for telehealth providers to maximize potential revenue sources, including payor reimbursement, to offset potential cost increases and to continue to financially support telehealth programs. At the same time, however, telehealth providers are facing increased OIG scrutiny of telehealth claims, requiring providers to take all necessary steps to develop and implement legally compliant billing practices as part of their overall compliance program.

Research and Innovation

US Food and Drug Administration

The Cures Act, signed into law on December 13, 2016, set a tone of innovation and increased access to digital health products in 2017. Under Commissioner Scott Gottlieb, the US Food and Drug Administration (FDA) maintained its commitment to digital health by continuing to address areas of

stakeholder uncertainty and perceived barriers to timely market authorization.

In July 2017, FDA published its Digital Health Innovation Action Plan, in which the agency acknowledged that the traditional regulatory approach toward moderate and higher risk medical devices is not well suited for the fast-paced, iterative design, development and type of validation used for digital health software products today. The FDA therefore announced its intent to explore an innovative approach to the regulation of digital health products that consists of three prongs: the implementation of the Digital Health Software Precertification (PreCert) Program, the issuance of new guidance, and an internal expansion of FDA's digital health capabilities.

A pilot of the PreCert Program was launched in September 2017 with nine software developers as participants. The purpose of the pilot is to develop a new "firm-based" approach toward regulating digital technology under which FDA's Center for Devices and Radiological Health (CDRH) could "pre-certify" eligible digital health developers that demonstrate "a culture of quality and organizational excellence" based on the objective criteria identified in the PreCert Program pilot. Then, pre-certified developers could, in theory, qualify to market their lower-risk devices without additional FDA review or with a streamlined premarket review. FDA indicated that it intends to leverage participant input to create this new and potentially faster regulatory pathway.

FDA also issued a number of guidance documents—some of which were promised in the Digital Health Innovation Action Plan—that affect digital health product development and compliance activities, analyses regarding the regulatory status of products in the United States, and the overall regulatory strategy for those products.

- On July 25, 2017, FDA took a key step toward easing restrictions on the secondary use of data and biospecimens in connection with FDA-regulated clinical investigations. FDA indicated in the "IRB Waiver or Alteration of Informed Consent for Clinical Investigations Involving No More Than Minimal Risk to Human Subjects" guidance (Waiver Guidance) that it will modify its position on requirements for institutional review board (IRB) waiver or alteration of informed consent. The development will likely have the effect of making it easier to use real world data in connection with FDA submissions and perform other FDA-regulated minimal risk data-driven research or research using leftover biospecimens.
    - The Common Rule and HIPAA include waiver provisions that would allow an investigator to use identifiable data or leftover biospecimens for research when it is impracticable to obtain consent (such as where the research involves the retrospective analysis of electronic health records of a significant number of individuals) and where other criteria are satisfied. In contrast, FDA historically did not allow waiver of informed consent except in cases of research of FDA-regulated products in emergency settings and investigations of *in vitro* diagnostics using leftover human specimens that are not individually identifiable.
    - Under authority granted to FDA in the Cures Act, FDA issued the Waiver Guidance indicating that it intends to revise its regulations regarding IRB waiver to align with those under the Common Rule. In the meantime, FDA has indicated it does not intend to object to the conduct of a minimal risk investigation for which an IRB waives or alters informed consent according to the framework outlined in the Guidance.
- On August 31, 2017, FDA issued the "Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices" final guidance (RWE Guidance). The RWE Guidance describes FDA's position that data derived from real-world sources may be used to support FDA regulatory decisions and clarifies the criteria by which FDA evaluates real-world data to determine whether the data is sufficient for generating the types of real-world evidence (RWE)

that can be used in regulatory decision-making. Notably, the RWE Guidance expressly maintains the "reasonable assurance of safety and effectiveness" evidentiary threshold that FDA-regulated devices must meet, but confirms that it is possible for RWE to satisfy this standard if the underlying data were generated at clinically relevant intervals throughout the device lifecycle and are otherwise reliable and appropriately validated.

- On October 25, 2017, FDA issued the "Deciding When to Submit a 510(k) for a Software Change to an Existing Device" final guidance (the 510(k) Guidance), which assists in determining when a software, including firmware, change to a device may require a manufacturer to submit a new 510(k) premarket notification. The purpose of the 510(k) Guidance is to increase the predictability, consistency and transparency of the "when to submit" decision-making process by outlining the applicable regulatory framework and guiding principles.
- On December 7, 2017, FDA published its highly anticipated "Clinical and Patient Decision Support Software" draft guidance (CDS Draft Guidance), which describes how the agency intends to exercise oversight over clinical decision support (CDS) and patient decision support (PDS) software. With the notable exception of the proposal to exercise enforcement discretion with respect to certain PDS software, the positions set forth in the CDS Draft Guidance—and the examples provided therein—mirror previous FDA guidance and examples that pre-dated the Cures Act.
- Simultaneously, FDA issued a draft guidance document that states how the agency intends to revise four previously issued digital health final guidance documents for consistency with the Cures Act, which amended the Federal Food, Drug and Cosmetic Act's definition of "device" to exclude software with several types of functions (including certain CDS functionalities). The changes proposed to these guidance documents primarily involve the movement of certain device functionalities from lists of products over which FDA intends to exercise enforcement discretion to lists of products that do not meet the definition of a device after the enactment of the Cures Act.
- Also on December 7, 2017, FDA released the International Medical Device Regulators Forum (IMDRF)-supported "Software as a Medical Device (SAMD): Clinical Evaluation" guidance document (SAMD Guidance). The purpose of the SAMD Guidance is to establish a common understanding of clinical evaluation and principles for demonstrating the safety, effectiveness and performance of SAMD. As with previously issued IMDRF guidance documents, the SAMD Guidance provides an evidentiary and technical framework that FDA intends to consider in the development of its regulatory approaches for digital health technologies.

Taken together, the Digital Health Innovation Action Plan and various FDA guidance statements continue to clarify how developers should approach certain development, classification and post-market product decisions and surveillance for digital health products in 2018. However, important questions remain unanswered, most notably the following:

- If FDA chooses to further pursue a precertification regulatory pathway for digital health software products, what might the pathway require of both developers and products?
- How will FDA regulate CDS software that relies on complex machine learning functionality?
- Will FDA issue specific guidance on the implementation of FDA's Medical Device Quality System Regulation for digital health products and software-based medical devices?

CDRH issued and prioritized the guidance documents that it intends to publish in FY 2018, which include the draft guidance "Multifunctional Device Products: Policy and Considerations." The guidance hopefully will clarify how FDA plans to regulate multifunction software products that provide multiple intended uses and both regulated and potentially unregulated functions.

FDA also plans to hire new staff for its Digital Health Program, including Entrepreneur-in-Residence (EIR) Fellows. New staff will work with "reviewers, compliance officers, and others within FDA to improve the quality, predictability, consistency, timeliness, and efficiency of decision making on individual products and firms," while EIR fellows will support various aspects of the PreCert Program development.

Supporting Digital Health Product Claims

As digital health companies continue to engage in research, development and testing of new products, they should be mindful of the need to understand and meet regulatory standards and user expectations for the evidence that supports their products in order to ensure compliance and promote commercial success. Notably, the New York Attorney General's office announced a settlement with the developers of three mHealth applications for, among other things, allegedly making misleading commercial claims. The settlement requires each developer to revise its advertising, consumer warnings and privacy practices and pay a monetary penalty to the Attorney General's office. The settlement underscores the importance of mHealth developers making a careful determination of when an app is subject to the jurisdiction of FDA (which requires labeling claims to be appropriately supported by clinical evidence) or state law, and if not so regulated, what evidence is necessary to satisfy the expectations of patients, consumers or other anticipated users in the health care industry and how such evidence can nonetheless be collected in accordance with applicable privacy and human subjects research requirements.

As evidenced by this settlement, regulators will hold technology companies accountable for ensuring that their product claims are supported by sufficient evidence. The research, development and testing that must occur to generate such evidence will require companies to continue to face the question of what regulatory, normative or other industry standards apply to such activities.

Modernization of Federal Human Subject Protection Regulations

HHS issued a long-awaited final rule amending the Common Rule (Common Rule Final Rule) in an effort to bring the human subject protection regulations into the modern, digital era. The regulation includes several changes designed to ease regulatory burdens on institutions that conduct human subjects research, particularly research involving secondary use of data and biospecimens. Notably, the regulation restricts the scope of the Common Rule to studies that are funded or supported by a federal signatory agency—*i.e.*, institutions may no longer voluntarily submit human subjects research that is not government funded to oversight by the Office for Human Research Protections.

The Common Rule Final Rule also includes a new exemption that provides for limited IRB review of the storage, maintenance and secondary use of identifiable data and biospecimens, where the investigator obtained broad consent that meets specific requirements under the Common Rule. It also introduced a new exempt category for research involving collection and analysis of identifiable health information when the use is regulated under HIPAA as research, health care operations or public health activities. Entities that constitute covered entities or business associates, or that seek to receive identifiable health information from such entities, will likely welcome the new exemption.

Digital health companies that interact with providers, patients and consumers, or that use personally identifiable information or identifiable health information to develop and refine their products and solutions, have long debated the extent to which they should incorporate the Common Rule into such activities. The normative significance of the Common Rule as it relates to digital health research continues to evolve with the issuance of the Common Rule Final Rule, and questions remain as to

whether companies will seek to incorporate its standards—some of which include less burdensome pathways for conducting human subjects research—into their research, development and testing activities.

Soon after the change in presidential administration, the White House announced that it was reviewing the Common Rule. As of the date of this publication, a final rule is undergoing review at the Office of Management and Budget to delay the effective date of the Common Rule Final Rule. Based on reports, there is no indication that the administration would make substantive changes to the regulation. Stakeholders should continue to monitor these developments, particularly because of the easing of regulatory burdens that the Common Rule Final Rule may bring for certain types of research.

Finally, HHS is expected to continue its efforts to implement directives under the Cures Act relating to research. In addition to initial guidance that OCR has issued on the topics of remote access under the HIPAA "reviews preparatory to research" pathway, HIPAA authorizations for future research, and revocations of research authorizations (which we intend to address in a separate publication), OCR is engaging in "additional research and discussions" on the issue of authorizations for future research and has suggested that additional guidance is forthcoming.

Artificial Intelligence & Machine Learning: Behind the Hype

In 2017, industry and trade press was dominated by reports on high-quality artificial intelligence (AI) and machine learning (ML) clinical applications, frequently still under development. While much of the hype focused on AI and ML capabilities in clinical settings, under-the-radar AI and ML applications were beginning to demonstrate their value in less dramatic ways, such as improving workflows and administrative functions, and creating efficiencies in research, development functions and other "back-office" settings.

Advances in AI and ML applications have also generated compliance uncertainty across a variety of industry and settings, including uncertainty about which legal and regulatory frameworks should apply to current and future iterations. Further, examples of poorly or inappropriately functioning systems garnered press attention in 2017, particularly in the area of bias. Despite these problems, 2017 saw no significant legal or regulatory changes focused on AI and ML outside of FDA. As was pointed out in a fall 2016 White House report on AI and ML, however, legal and regulatory changes to accommodate AI and ML require significant research to achieve the appropriate balance among multiple concerns, including safety, allocation of risk and support for innovation.

While resolution of some of the more esoteric issues relating to AI and ML applications in health care delivery may remain years away, it is possible that medical boards, medical societies and schools of medicine may soon begin to seriously consider the impact of these technologies on care delivery. Just as these bodies have struggled with how to most effectively embrace new technologies such as telemedicine, they will turn their attention to AI and ML. Whether serious attention is paid in 2018 remains to be seen.

So, what did we learn in 2017?

Data, Data, Data

The availability of troves of data catalyzed the growth of AI and ML. But the ownership, storage, use, disclosure, quality and curation of data often present unique legal and regulatory obligations in the

health care sector, resulting in unanticipated challenges to the use of health data. Stakeholders—data sources, software developers, clinicians recommending software and consumers—should be cognizant of when, where and how data may be appropriately used and transferred under applicable federal and state laws. Users of health data also must be aware of the risk of bias, either in the data sets themselves or in the data methodology. Consistency in curation in data sets is also critical to appropriate functioning.

While the legal and regulatory risks associated with these matters may not be clear in all circumstances, the failures of an AI system can be subjected to analysis under existing theories, such as negligence or product liability, and in the future we should expect legislatures and perhaps courts to deploy new theories. Further, the practical consequences of these failures can include significant reputational risk, particularly in an industry in which sensitive personal information is used to develop new therapies. Ownership of certain intellectual property rights in the data, including rights in compilations, and the appropriate licenses to use that data, may also create pitfalls.

Key FDA Considerations

In late 2016, the Cures Act amended the Federal Food, Drug and Cosmetic Act's definition of "device" to exclude several types of software that could include AI or ML applications. The Cures Act identified four criteria required for the exemption:

1. Not intended to acquire, process or analyze a medical image or a signal from an *in vitro* diagnostic device or a pattern or signal from a signal acquisition system
2. Intended for the purpose of displaying, analyzing or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines)
3. Intended for the purpose of supporting or providing recommendations to a health care professional about prevention, diagnosis or treatment of a disease or condition
4. **Intended for the purpose of enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient**

To meet the exemption, the software product must not be intended to serve as the sole basis for a diagnostic or treatment decision. FDA regulates the manufacture and distribution of products intended to be utilized for the diagnosis, treatment, and cure or prevention of disease or other conditions—*i.e.*, medical devices. Prior to the adoption of the Cures Act, FDA had promulgated a number of guidance documents related to digital health tools and, as noted previously, in 2017 FDA updated some of the guidance to take into account the new law. While some media and trade reports suggest that uncertainty remains regarding if and how FDA will and should regulate AI and ML products, the guidance, existing regulatory framework and recent device clearances make clear that FDA intends to regulate AI and ML tools that provide diagnostic, clinical and medical device functions that fall within FDA's jurisdiction.

As FDA clears and approves innovative products, stakeholders may identify trends that indicate the perceived risk profile of functionalities and types of software that serve more as a physician than supporting software in care delivery. As referenced previously, if finalized in 2018, FDA's new precertification pathway for software products may present an interesting opportunity to commercialize a greater number of products, potentially faster.

Beyond FDA

The requirement for FDA clearance of a medical device does not necessarily limit physician utilization of a product for off-label purposes. Further, devices that do not fall within FDA oversight, such as qualifying CDS and PDS software, do not even include the imprimatur of FDA oversight. Instead, these devices are regulated by an array of laws and regulations that must be navigated by developers, consumers and providers of health care services. State medical boards, which regulate the practice of medicine to ensure that the physician community is adhering to appropriate standards of care, can play a role, as can medical societies, which provide advice regarding best practices. Ultimately, the standards applicable to AI and ML applications in the clinical setting will be tested by theories of negligence utilized by plaintiffs in civil cases.

FUTURE of AI Act

While it is likely that the Republican-controlled Congress will continue to focus on its broader agenda, it is possible that Congress will take action on the FUTURE of AI Act. This Act, which has been introduced in both the House and the Senate, would establish a committee to advise the Secretary of Commerce on AI in the context of a variety of issues, including work force, education, legal and regulatory regimes, and international competitiveness. If the FUTURE of AI Act becomes law, the United States would join a growing list of nations, including the United Kingdom, that are actively engaged in understanding the broad implications of AI and ML. Such an effort could easily affect the development of AI and ML applications in health care.

Privacy

Issues related to data privacy and security show no signs of diminishing, and their impact on AI and ML applications remains to be seen. Nonetheless, these issues likely will continue to raise perplexing issues for stakeholders.

Attorneys Lisa Schmitz Mazur, Vernessa T. Pollard, Michael W. Ryan, Dale C Van Demark and Scott A. Weinstein also contributed to this post.

National Law Review, Volume VIII, Number 9