MINTZ

Telehealth, Health IT, and mHealth Policy: Considerations for Stakeholders

January 06, 2015 | Alert | By **Alexander Hecht**, Andrew Shin

VIEWPOINT TOPICS

- ML Strategies

RELATED PRACTICES

RELATED INDUSTRIES

In recent months, as the conversation about reforming the health care system has shifted from websites and coverage expansion to achieving greater delivery system efficiencies, cost containment, and quality improvement, the role of health care technology — specifically, telehealth, health information technology (health IT or HIT), and mHealth — is becoming an even more prevalent area of bipartisan cooperation among health care policymakers.

In the 113th Congress there was a proliferation of policy and industry attention on telehealth, health IT, and mHealth as lawmakers and stakeholders alike have recognized the cost, quality, and accessibility benefits of telehealth and momentum for implementation of telehealth are growing. For example, at least **57 bills** that relate to telehealth were introduced. Representative Fred Upton, Chairman of the House Energy and Commerce Committee, embarked on a "21st Century Cures Initiative," and convened a series of hearings and roundtables with the ultimate goal of developing legislation to promote innovation in the health care space.

In the 114th Congress, there is reason to believe the momentum for policy to address telehealth will only continue, if not increase in pace. With the current Medicare Sustainable Growth Rate (SGR), or "Doc Fix," set to expire in March 2015, lawmakers are expected to once again turn their attention to SGR reform in the lame duck. This focus on overhauling the physician payment formula, and more broadly payment reform, will likely also drive continued attention to telehealth reimbursement challenges, discussed in more detail below.

Telehealth: Rising Momentum

The progression of telehealth in recent years is perhaps best demonstrated by a recent report finding that the number of patients worldwide using telehealth services is expected to grow from 350,000 patients in 2013 to approximately 7 million by 2018.[1] Moreover, three-fourths of the 100 million electronic visits expected to occur in 2014 will occur in North America.[2]

The growing demand for telehealth services reflects the important role telemedicine plays in reducing costs while also increasing quality, access, and satisfaction. A June 2014 American Medical Association (AMA) report notes that telehealth is being used to "improve access to care, care coordination and quality, as well as reduce the rate of growth in health spending."[3] For example, it is estimated that telehealth could deliver more than $6 billion a year in health care savings to U.S. companies[4] and that it yields an 87 percent satisfaction rate.[5]

Regulatory Landscape and Barriers to Telehealth Proliferation

While telehealth is poised to address some of the most challenging problems in the U.S. health system, there are still significant barriers to deployment.

> ❝
>
> *Reimbursement*
>
> **Current federal law is extremely restrictive on how telehealth is paid for — resulting in a disincentive to provider adoption. For example, Social Security Act Section 1834(m) defines the**

conditions for payment for telehealth services under Medicare. The statute requires that a patient must present at a rural, clinical originating site in order to receive care via telehealth. Thus, Medicare reimbursement for telehealth is only available at clinical sites in rural areas and patients seeking care in metropolitan areas are unable to access these services. These restrictions have led to extremely low Medicare reimbursement for telehealth encounters, with only a reported $11.8 million for calendar year 2013.[6] Modernizing the regulatory framework for Medicare telehealth reimbursement in a way that is mindful of reducing and not increasing the overall cost of Medicare will almost certainly be a primary focus of upcoming Congressional action.

While almost every state has a Medicaid plan that covers at least some telehealth services, coverage across states varies greatly and many states follow Section 1834(m) in its restrictive language. Still, states are moving toward greater adoption of telehealth services. For example, according to the American Telemedicine Association (ATA), in 2014 15 states[7] proposed legislation mandating private coverage for telehealth while 11 states[8] proposed legislation mandating Medicaid coverage for telehealth.

In addition, CMS updates telehealth payment policies in its yearly physician payment rule. In its recent final CY 2015 rule, CMS included new billing codes for telemedicine services for which providers can bill Medicare. These new Current Procedural Terminology (CPT) codes include telemedicine reimbursement for psychoanalysis, family psychotherapy, and annual wellness visit exams.

Finally, the 2014 CMS Physician Fee Schedule Rule established a policy to make separate payment for non-face-to-face chronic care management (CCM) services for Medicare beneficiaries who have multiple and significant chronic conditions (two or more). For CY 2015, CMS finalized a rule on October 31st to:

- Set a payment rate of $41.92 for the CCM code. This code may only be billed once per month.
  - Allow more flexibility in the supervision of clinical staff providing CCM services.
    - Not establish separate standards for these services, as proposed last year.
- Suggest standards for electronic health records and whether additional standards are needed.

The change in supervision requirements means that physicians and other practitioners would be able to employ clinical staff either directly or under contract, and could provide general supervision at all times, not just after hours. The benefit to telehealth is that there are no additional standards required to provide CCM and the establishment of a payment rate. In essence, CCM, and now the reimbursement amount associated with it, represent another service offering that could utilize telehealth services, and it would introduce another opportunity for physicians to utilize telehealth services, where possible.

Notably, in a proposed rule released December 1st to strengthen the Shared Savings Program for Accountable Care Organizations (ACOs), CMS proposed to give ACOs "flexibility to use telehealth services as they deem appropriate for their efforts to improve care and avoid unnecessary costs."[i] While the rule stops short of waiving Medicare requirements in telehealth entirely, it is a positive step towards additional access to telehealth services.

Clinical Permissibility – Defining Telehealth

Currently, there is no federal standard for clinical guidelines in telehealth; medical boards and state regulatory boards across the country are each responsible for setting the standards for the appropriate practice of medicine via telehealth in their state. This has resulted in a patchwork of state laws that inhibit the proliferation of telehealth solutions in both the public and private sectors.

As of June 2013, 40 out of 50 states have introduced legislation addressing telehealth policy. There is wide variation in how telehealth is defined and treated — leading to ambiguity and uncertainty on such key questions as whether a treatment relationship between a health care provider and patient may be established online; what the standard of care for online encounters should be; the conditions for ensuring safe online prescribing through telehealth; and ensuring privacy and the security of patient records.

Efforts in Congress to modernize the regulatory treatment for telehealth will likely address the issue of how to actually define telehealth. One option might be for Congress to defer this authority to the Administration to create a definition through a public, multi-stakeholder process — for instance, either a notice and comment rulemaking or a sub-regulatory guidance document. Republicans, however, given their distrust of the current Administration, might not be inclined to provide HHS this authority. Other alternatives for a telehealth definition could include:

- **Existing Public Health Service Act (PHSA) Definition.** The PHSA defines the term "telehealth" as "the use of electronic information and telecommunications technologies to

support long distance clinical health care, patient and professional health-related education, public health, and health administration."9 Some stakeholders believe this definition is broad and technologically neutral, while others have issues with terms like "long distance" and believe that it is ambiguous and not specific enough to fully capture all telehealth use cases.

- **Federation of State Medical Board (FSMB) Definition of Telemedicine.** In April 2014, the FSMB finalized a new *Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine*.10 The new model policy defined "telemedicine" as "the practice of medicine using electronic communications, information technology or other means between a licensee in one location, and a patient in another location with or without an intervening healthcare provider. Generally, telemedicine is not an audio-only, telephone conversation, e-mail/instant messaging conversation, or fax. It typically involves the application of secure videoconferencing or store and forward technology to provide or support healthcare delivery by replicating the interaction of a traditional, encounter in person between provider and a patient."

This FSMB model policy should be influential as medical boards across the country look to modernize their regulatory definitions for acceptable telemedicine. Some stakeholders have expressed concerns by what they perceive to be a bias in the definition against telemedicine conducted by telephone, and are concerned that the FSMB's definition may suppress future innovation.

- **Telehealth Modernization Act (H.R. 3750) Definition.** Another potential definition for telehealth is contained in the Telehealth Modernization Act, introduced in the 113th Congress by Representatives Doris Matsui (D-CA) and Bill Johnson (R-OH). This bipartisan measure defines telehealth as "health care that a health care professional is authorized to deliver to an individual in person under State law, such health care delivered by such health care professional to such individual not in person, from any location to any other location, and by means of real-time video, secure chat or secure email, or integrated telephony." The Telehealth Modernization Act is supported by a wide range of telehealth technology providers and health industry stakeholders, including Health IT Now, America's Health Insurance Plans (AHIP), and the Blue Cross Blue Shield Association (BCBSA).

Licensure

As with clinical permissibility, licensure is set on a state-by-state basis by state medical boards — and a provider typically must be licensed in the state in which a patient is located when receiving the treatment. With the advent of telehealth, licensing of health providers must be updated to reflect the flexibility provided by telehealth — allowing health care experts to bring their expertise virtually to where it is needed, even across state borders.

There have been several solutions floated to address the problem of licensure. For example, the FSMB is also attempting to tackle licensure, with its *Interstate Licensure Compact*. FSMB released a draft of this document in 2014.11 The compact is intended to "develop a comprehensive process that complements the existing licensing and regulatory authority of state medical boards, ensures the safety of patients, and enhances the portability of a medical license, providing a streamlined process that allows physicians to become licensed in multiple states." The FSMB released a final version of its licensure compact on August 5th. Now that the drafting process is complete state legislatures and medical boards can begin to consider adoption.

As with other aspects of telehealth policy, legislation has already been introduced in Congress to address the issue of licensure. For example, H.R. 3077, the Telemedicine for Medicare (TELE-MED) Act, discussed further below, would allow treatment under Medicare via telehealth across state lines. There is significant support for the measure, demonstrated by an industry letter with 66 stakeholder signatories; however, concerns remain regarding professional accountability and cross-state practices.

At its recent interim meeting of the House of Delegates, the American Medical Association (AMA) adopted new policies supporting the interstate compact developed by the FSMB. Under this policy, "AMA will work with medical associations, FSMB, and other interested stakeholders to ensure expeditious adoption of the compact and the creation of an Interstate Medical Licensure Commission."ii The AMA also approved new policy to support paying for telemedicine services for patients who have difficulty accessing specialists, even if patients are not in shortage areas.

State Landscape

Addressing a number of the challenges discussed above, the American Telemedicine Association (ATA) released two policy reports in September 2014 grading states and seeking to identify gaps in coverage and reimbursement, and in physician practice standards and licensure. The reports, which present a 50-state snapshot of telehealth policy, shed light on a complex regulatory landscape and highlight the differences in state policies. The first report compares coverage and reimbursement standards among states, revealing increasing telemedicine utilization. The second report, dealing with physician practice standards and licensure for telemedicine, reviews

Recent Telehealth Policy Advancements

As discussed above, 57 bills were introduced that deal with telehealth. An ML Strategies spreadsheet detailing these bills can be found **here**. Moreover, last Congress the House Energy and Commerce Committee's 21st Century Cures Initiative is exploring how Congress can facilitate telehealth innovation and adoption. To date, the Committee has held nine hearings and roundtables and floated four white papers to support this initiative. As part of this effort, the Committee is planning to develop legislation to reflect, harness, and promote innovation occurring in the health care space. The Committee is actively seeking comments and ideas on this initiative and on legislation. This could be a timely moment for telehealth providers to make their voice heard in Congress and develop policies that will allow the broader deployment of telemedicine.

In addition to the Committee's 21st Century Cures Initiative, several key pieces of legislation have been introduced that address some of the most pressing aspects of telehealth policy, including clinical permissibility, licensure, and reimbursement.

In addition to the bills discussed above, Representatives Mike Thompson (D-CA), Glenn Thompson (R-PA), and Peter Welch (D-VT) recently introduced **H.R. 5380**, the Medicare Telehealth Parity Act of 2014. The bill would expand specific telehealth services under Medicare in two-year increments over three phases, including to the home. This proposal represents a more incremental, phased in approach to expansion of Medicare reimbursement for telemedicine encounters — designed to keep the overall cost of the bill down. In particular, the Thompson bill would provide new opportunities for reimbursement of telehealth and remote monitoring technologies under Medicare. This bill will likely be included in the mix of proposals that the House Energy and Commerce Committee considers as it crafts the health care technology component of the 21st Century Cures Initiative.

With the Senate Health, Education, Labor, and Pensions Committee planning to begin an effort similar to the House 21st Century Cures Initiative, the Senate has also focused in on telehealth. In September 2014, the Senate Special Committee on Aging held a **roundtable** titled, "Harnessing the Power of Telehealth: Promises and Challenges?". Panelists representing Federal agencies including CMS, the Federal Trade Commission (FTC), and Federal Communications Commission (FCC), industry, and stakeholder groups discussed licensure, reimbursement, and how to define telehealth.

In addition to Congressional advancements, outside stakeholders have laid out best practices for telehealth policy initiatives.

In June 2014, the AMA approved a report, *Coverage of and Payment for Telehealth*, which provides an overview of telemedicine and establishes AMA policy toward telehealth. The report includes principles such as, for example, that a valid patient-physician relationship can be established face-to-face through the use of real time audio and video technology. It also provides that patients seeking care via telemedicine must have a choice of provider; both the patient and physician should be clearly identified in advance; and telehealth encounters should be properly documented, abide by laws addressing the privacy and security of patients' medical information, and be delivered in a transparent manner.12

As discussed earlier, the FSMB policy also establishes that treatment made in an on-line setting should be held to the same standard of appropriate practice as those in traditional settings. It clarifies that a treatment relationship can be established online; creates online prescribing safeguards; and ensures telehealth encounters are HIPAA compliant and include informed consent, generate medical records, and support continuity of care.

Telehealth and Communications Technology

Telehealth represents the unique intersection of health care and communications technology. While, in itself, telehealth is a valuable tool, it cannot exist in a vacuum and will rely on communications and technology infrastructure to reach its full potential.

The FCC plays a role in building the wired and wireless foundation that telehealth will need to be implemented in the most valuable manner. Currently, the FCC's Rural Health Care Program "provides funding to eligible health care providers for telecommunications and broadband services necessary for the provision of health care."iii The program is made up of three sub-initiatives, including: the **Healthcare Connect Fund**, the **Telecommunications Program**, and the **Rural Health Care Pilot Program**. Among other things, these programs make available $400 million in annual funding to increase broadband access for health care professionals.

In addition to driving broadband adoption, the FCC is responsible for allocating wireless spectrum and equipment authorization. For example, the FCC recently updated its 2012 rulemaking governing allocation of spectrum to wearable medical sensors, known as Medical Body Area Networks (MBANs), which transmit patient data to a control device. The updates provide additional flexibility for implementation of

standards for MBAN devices and clarify the rule's treatment of deployment for these systems. In 2013, the FCC also passed an experimental licensing order, allowing spectrum users — including those with medical device and remote monitoring services — to promote expanded opportunities for radio experimentation in broadband and licensing trials.

Health IT

Since the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, the proliferation of the health information technology (HIT) industry and regulations governing it have exploded. Policies have spanned from federal mandates such as those setting up the meaningful use incentive program ("meaningful use") to state and regional regulations with regard to health information exchange. In some cases, like the much anticipated switchover to the new ICD-10 coding system, stakeholders and regulators were left waiting for at least another year as Congressional lawmakers quietly inserted a delay during negotiations around Medicare physician payment. In another circumstance, the Obama Administration signaled its forward-looking objective in the coming months to devise a roadmap for the future of interoperability.

As stakeholders await finalization of the Meaningful Use 2 guidelines in addition to regulation over mHealth devices and clinical decision support applications, there is still a great deal of activity anticipated through the Office of the National Coordinator for Health Information Technology (ONC), the lead office in the Obama Administration for HIT matters, and also the Food and Drug Administration (FDA) among other agencies and offices outside the Department of Health and Human Services (HHS), including the FCC and the FTC.

What's Ahead for HIT?

ICD-10: Although many stakeholders were surprised by the one-year delay embedded in the Medicare Sustainable Growth Rate patch bill, also known as the "Protecting Access to Medicare Act of 2014," most health policy experts believe the cost for ICD-10 adopters would grow too high if lawmakers instituted an additional delay. On July 31, 2014, HHS released a **rule finalizing October 1, 2015** as the new compliance date for health care providers, health plans, and health care clearinghouses to transition to ICD-10. To take advantage of the delay, HHS is administering a series of training opportunities to be fully prepared for the new transition date, which could offer stakeholders ample opportunities to engage policymakers as problems arise.

FDA Oversight: Many HIT vendors and app developers have feared a possible overreach from federal regulators from even before passage of the HITECH Act in 2009. After a series of ambiguous and expansive statements, regulators from multiple agencies issued their clearest guidance to date on April 3, 2014 via a report entitled, ***Proposed Strategy and Recommendations for a Risk-Based Framework***. The report proposed a strategy and recommendations for regulation of health IT that identifies and distinguishes between three types of health IT: (i) administrative health IT; (ii) health management health IT, and (iii) medical device health IT. The distinction between these three categories represented policymakers' intent to focus on the functionality of a particular product — rather than the platform — as a means for determining the relative risks and determining the appropriate recommendations. Following a public meeting and comment period, stakeholders are hoping that regulators finalize the rule, along with additional clarification and also explicit exemptions from the regulatory framework.

Already, **the FDA issued a notice on August 1, 2014** that exempted dozens of mHealth medical devices from regulatory oversight. The FDA proposed eliminating the need for premarket submission requirements from certain Class I and II medical devices under the reserved criteria of section 501(I) of the Federal Food, Drug and Cosmetic Act of 2012. Stakeholders now await further guidance in other categories ranging from distinguishing wellness versus clinical tools and the treatment of certain clinical decision support apps.

Meaningful Use: Recent data has indicated that while a majority of hospitals in the United States have an Electronic Health Record (EHR) system, less than six percent of them would be able to meet all the requirements in the original Meaningful Use 2 regulation. On August 29, 2014, **CMS released a proposed rule** that would offer more flexibility for adopters by using the 2011 edition of certification criteria in 2014 and also formalizing the intent to extend Stage 2 to 2016 and to begin Stage 3 in 2017. In addition, stakeholders are anticipating further efforts from CMS to align reporting and submission requirements between the Medicare meaningful use and the Hospital Inpatient Quality Reporting program.

Interoperability: The seamless exchange of health care information has been a goal and persistent struggle from the onset of the health information era. The efforts from industry stakeholders and policymakers alike to identify and remove barriers to interoperability while aligning regulatory frameworks have been exacerbated as the adoption of HIT increases. ONC has been under way over the past year on a multi-stakeholder listening tour of sorts to create a consensus-based framework that is achievable and effective.

Independent Federal Advisory Committees like the **JASON Taskforce and Interoperability and Health Information Exchange – Governance Subgroup**, have held a series of meetings and issued multiple reports on challenges to achieving interoperability. Additionally, ONC itself released two reports over the past year (**Connecting Health and Care for the Nation: A 10-Year Vision to Achieve an Interoperable**

Health IT Infrastructure and **HHS Principles and Strategy for Accelerating Health Information Exchange**) in addition to hosting its own, interactive **community**. All this feedback will be integrated into a report that is expected to be published in early 2015. Dr. Karen DeSalvo, the former head of the ONC, has indicated that the report would be the first version of a nationwide interoperability roadmap and a plan for achieving three, six, and ten year interoperability milestones. The ONC Health IT Policy and Standards Committee is meeting on October 15th to discuss the IMC interoperability roadmap and JASON Taskforce recommendations for EHR interoperability.

Data Security: Data breaches cost the health care system at least $5.6 million per year and account for almost half of all major breaches according to industry experts. However, with the acceleration of digitizing data as well as improving data accessibility through the exchange of electronic health records, data security has quickly become one of the top issues facing policymakers this year. Additionally, the volume of data points collected and stored continues to increase as various payment systems demand providers report more patient data through various initiatives such as the Medicare Physician Quality Reporting System (PQRS).

Adding to the complex environment is the estimated 90 million wearable data devices (WDD) that will be shipped to customers in 2014. A Mintz Levin alert on WDDs can be found **here**. Aside from possible FDA safety and effectiveness oversight, these devices will further expose consumers and even employers to the threat of data breaches and privacy concerns among other issues. Experts and policymakers alike have increased calls for legislative action ranging from more FTC authority to impose safety standards and consumer notification rules to calls to update the landmark privacy law, HIPAA, to account for current technologies and uses of health care data.

mHealth

Health IT and medical software, especially those utilizing mobile technology such as tablets, smartphones, and wearables, known as mHealth, have seen tremendous growth in the past few years. National health reform efforts and the increased scrutiny that highlighted the inefficiencies of the delivery system, and renewed focus on personal health/wellness, helped to accelerate growth in the budding market for technologies that assisted clinicians in evidence-based protocols and care coordination to personal devices that track physical activity and other bodily measurements.

Initial FDA Regulation of mHealth

Last year, industry stakeholders including medical device manufacturers, software developers, the communications/wireless industry, electronic health record companies, patient groups, and many others were intensely focused on the initial framework for FDA oversight and regulation of mHealth technology. In September 2013, the FDA published final guidance outlining a "tailored approach" that instituted nonbinding recommendations for mobile medical apps that meet the definition of "device" under the Federal Food, Drug, and Cosmetic Act and are intended to be used as an accessory to a regulated medical device, or to transform a mobile platform into a regulated medical device.[iv]

The FDA indicated that it would exercise "enforcement discretion" and would not regulate apps that pose minimal risk to patients and consumers, including apps that helped patients/users self-manage their disease or condition without providing specific treatment suggestions or that enabled patients or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems.

Instead, the FDA stated that it would focus on apps that presented a greater risk to patients and consumers if they fail to work as intended, such as apps that used a sensor or lead that is connected to a mobile platform to measure and display the electrical signal produced by the heart (electrocardiograph or ECG) or that used an attachment to the mobile platform to measure blood oxygen saturation for diagnosis of specific diseases or conditions. The FDA determined that they would use the same regulatory standards and risk-based approach that the agency applies to other medical devices when assessing mobile medical apps that are subject to agency review.

Risk-Based Framework for Health IT

In April 2014, the three federal agencies charged with regulating health information technology — the FDA, ONC, and the FCC — issued a long-awaited ***Proposed Strategy and Recommendations for a Risk-Based Framework*** report.[v] The report proposed a strategy and recommendations for regulation of health IT that focused on the potential risks while promoting innovation, protecting patient safety, and avoiding regulatory duplication.

Congress mandated the development of the Report as part of the 2012 Food and Drug Administration Safety and Innovation Act ("FDASIA"), which required the Agencies to coordinate their efforts to regulate health IT and to develop and post a report on their websites to further such a framework.

The report recommended an approach to foster the development of a culture of safety and quality, leverage standards and best practices, employ industry-led testing and certification, and selectively use tools such as voluntary listing, reporting, and training to enable the development of a health care environment that is transparent and promotes learning and continual health IT improvement.

Importantly, the agencies did not call for additional regulation, stating that "we do not believe that regulation should be or needs to be the first approach used to reach this outcome." Rather, the report suggested the adoption of a limited, narrowly tailored approach that primarily relies on ONC-coordinated activities and private sector capabilities, and that a non-governmental, independent program may be effective in monitoring compliance. The recommendations in the report included continued interagency cooperation and collaboration, the creation of a public-private safety entity — the Health IT Safety Center — and a risk-based approach to the regulation of health IT.

To guide the analysis of the appropriate amount of oversight, the report identified and distinguished between three types of health IT:

1. **administrative health IT** (products for billing and claims processing, scheduling, and inventory management);

2. **health management health IT** (e.g., products for health information and data exchange, some clinical decision support products, provider order entry products, and electronic access to clinical results); and

3. **medical device health IT** (e.g., products for detection/diagnostics and remote monitoring). The distinction between these three categories represents the Agencies' intent to focus on the functionality of a particular product — rather than the platform (e.g., on-premises, web-based, mobile application, etc.) — as a means for determining the relative risks associated with these products and determining the appropriate recommendations.

The report also set forth a framework for regulation of health IT that applies mainly to health management health IT. The Agencies concluded that administrative health IT functionalities posed limited or no risk to patient safety and therefore did not require additional oversight. With respect to medical device health IT, the Agencies noted that medical device health IT was subject to greater oversight through FDA regulations that already focused on the functional risks of these products, and as such, "no new or additional areas of FDA oversight are needed."

The report described a framework based on the following four key areas,

1. *Promoting the use of quality management principles:*

2. *Identifying, developing, and adopting standards and best practices:*

3. *Leveraging conformity assessment tools;* and,

4. *Creating an environment of learning and continual improvement:*

Additionally, the report set forth much needed guidance on clinical decision support ("CDS") products. CDS products provide health care providers and patients with information to improve health and health care, such as computerized reminders and alerts for providers and patients. The report concluded that *most* CDS functionalities can be categorized as health management health IT and therefore would not be subject to FDA regulation. However, certain types of CDS tools that present higher risks to patients, such as computer-aided detection/diagnostic software, warrant FDA's continued oversight as medical device health IT. The FDA will work with federal and private stakeholders to clarify the types of medical device CDS that should be the focus of FDA's oversight.

With respect to the CDS products that fall within the health management health IT category, the Agencies recommended that health IT stakeholders work together to develop policies for the transparent disclosure of the rules and information sources underlying CDS products.

For more detailed analysis of the Risk-Based Framework, please read our **Mintz Levin Alert**.

Legislative Action Ahead

Following the passage of the Affordable Care Act (ACA), Congress has passed minimal legislation in the health care sector due to some influential members of the GOP who have only focused on complete repeal of the health reform law versus Democrats who have been wary of providing any opening to Republicans to fix/add to the law, fearing those efforts would serve to dismantle essential elements.

Yet, in a few instances, both parties have shown a willingness to deviate from ACA politics and respond to stakeholder concerns that require regulatory clarity in some cases or relief in others. Just recently, on December 4, 2014, Senators Michael Bennet (D-CO) and Orin Hatch (R-UT) introduced bipartisan legislation that would exempt low-risk medical software and mobile apps from FDA regulation. The Medical Electronic Data Technology Enhancement for Consumers' Health (MEDTECH) Act builds on the risk-based approach taken by the FDASIA workgroup last spring.[vi] The key element concerns clinical decision support software, which is often part of electronic health records and provides prompts to physicians based on research-based algorithms.

The language of the bill, which will be reintroduced in the 114th Congress, clarifies that FDA would regulate such software only if it automates the clinician's decision rather than just providing guidance. Software companies that make decision support have pushed for such a rule and have been waiting for FDA guidance since 2011.

The MEDTECH Act follows in the footsteps of similarly aligned legislation, mostly focused on removing and/or clarifying FDA oversight over health IT. On June 19, 2014, Senators Deb Fischer (R-NE) and Angus King (I-ME) introduced the Preventing Regulatory Overreach To Enhance Care Technology ("PROTECT") Act aimed at offering a regulatory framework for health IT innovation, while balancing patient safety protection.[vii] The bill and its companion in the House introduced by Representative Marsha Blackburn (R-TN) would remove some high-risk clinical decision support (CDS) software, mobile medical apps, and other medical device functionality from FDA oversight. Instead, FDA would prioritize technologies that posed the greatest health risk.

Among the list of high-risk CDS software that would no longer be regulated by FDA under the PROTECT Act:

- Apps and other software that guide untrained users to make very complex medical decisions — for example, consumer-use melanoma apps, sports concussion injury apps, drug dose calculators, and disease managers for patients;
- Software used in a setting that does not allow a doctor sufficient time to second-guess the software — emergency care predictive analytics software and hospital patient monitoring software; and
- Software that takes a very complicated calculation and presents a result without transparently revealing the basis for the calculation

Moving Forward

The landscape for mHealth regulation will likely grow in complexity as the sophistication and application of new technologies continues to expand to areas previously unthinkable by regulators. As wearables become implantables and as technology further bridges health care providers and suppliers with individuals in their homes and at work, innovation will continue to outpace regulation. Although that presents a risky proposition for some investors and entrepreneurs in the mHealth space and Health IT writ-large, it also means that there will be a renewed focus from policymakers wishing to provide clarity and fuel for the fire of innovation.

The **health care and life sciences team at ML Strategies** has been very active in the telehealth, health IT, and mHealth policy spaces and works closely with Congress and the Administration. Given the amount of activity taking place, we have put together this alert to highlight current opportunities for stakeholders to consider. We are available to discuss the contents of this alert further and to answer any questions.

Endnotes

1 HIS Abstract. A Dedicated Study on Telehealth that Provides Detailed Analysis of the World Market

2 Deloittee. "eVisits: the 21st century housecall." July 2014.

3 AMA. Report of the Council on Medical Service. Coverage of and Payment for Telemedicine. CMS Report 7-A-14. June 11, 2014.

4 Towers Watson's 2014 Health Care Changes Ahead Survey.

5 Intel. "Intel Study Reveals Telehealth Will Dramatically Transform Health Care: Experts See Telehealth as Essential to Managing Aging Population, Voice Need for Improving Reimbursement." May 18, 2010.

6 Center for Telehealth and e-Health Law (CTeL). "CMS Medicare Reimburses Nearly $11.8 Million for Telemedicine in 2013." April 28, 2014.

7 Alaska, Connecticut, Florida, Illinois, Iowa, Massachusetts, Nebraska, New Jersey, New York, Ohio, Pennsylvania, Rhode Island, South Carolina, Washington, West Virginia.

8 Iowa, Louisiana, Massachusetts, Missouri, New Jersey, New York, Oklahoma, Rhode Island, Washington, West Virginia.

9 42 U.S.C.S. 254c-16.

10 Federation of State Medical Boards. "Interstate Medical Licensure Compact." May 5, 2014.

11 AMA. Report of the Council on Medical Service. Coverage of and Payment for Telemedicine. CMS Report 7-A-14. June 11, 2014.

12 FSMB. "Model Policy for the Appropriate Use of Telemedicine Technologies in the Practice of Medicine." April 2014.

i CMS. Medicare Program; Medicare Shared Savings Program: Accountable Care Organizations. RIN 0938-AS06 http://www.ofr.gov/OFRUpload/OFRData/2014-28388_PI.pdf

ii AMA Adopts New Policies to Improve Health of Nation at Interim Meeting

http://www.ama-assn.org/ama/pub/news/news/2014/2014-11-20-ama-policies-improve-health-of-nation.page

iii Federal Communications Commission. Rural Health Care Program.
http://www.fcc.gov/encyclopedia/rural-health-care

iv FDA. Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM2

v Office of the National Coordinator for Health IT. FDASIA Health IT Report: Proposed Strategy and Recommendations for Risk-Based Framework.
http://www.healthit.govsites/default/files/fdasiahealthitreport_final.pdf

vi Medical Electronic Data Technology Enhancement for Consumers' Health (MEDTECH)
http://www.hatch.senate.gov/public/index.cfm/releases?ID=750a5957-08e0-4a77-95ba-5806a7f3ffa7

vii Preventing Regulatory Overreach To Enhance Care Technology Act of 2014.
http://www.fischer.senate.gov/public/_cache/files/7b25f3a3-2d8b-4638-aba9-b12cc68fde0d/tam14031.pdf

Authors
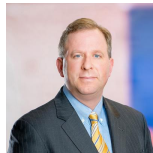
Alexander Hecht, ML Strategies - Executive Vice President & Director of Operations

Alexander Hecht is Executive Vice President & Director of Operations of ML Strategies, Washington, DC. He's an attorney with over a decade of senior-level experience in Congress and trade associations. Alex helps clients with regulatory and legislative issues, including health care and technology.

Andrew Shin

More Viewpoints

Wearable Devices in the Workplace Challenge Data Security and Privacy

August 21, 2014 | Advisory | By Jonathan T. Cain
Read more