CLIENT ALERT

Digital Health — Recent Developments (June 2016)

Jun.23.2016

In this alert:

Important Upcoming Dates:

1. **June 26-28, 2016** – Long-Term and Post-Acute Care Health IT Summit (Reston, VA). Crowell & Moring's own Jodi Daniel will be speaking at the event.
2. **June 27, 2016 by 5:00 p.m.** – Comments due regarding the MACRA proposed rule.
3. **July 8, 2016** – Application deadlines for High Impact Pilots (HIP) Awards and Standards Exploration Awards (SEA) programs.
4. **July 18, 2016** – Comments due regarding FDA guidance on the use of EHR data in clinical trials.
5. **September 8, 2016** – Submission deadline for Phase 1 of the Move Health Data Forward Challenge.

FTC Releases Proposed Settlement in Deceptive Business Practices Suit Against EHR Company

On June 8, 2016, the Federal Trade Commission (FTC) made public the terms of a proposed deceptive practices settlement with electronic health records (EHR) company Practice Fusion, Inc. The suit alleges that for over a year, Practice Fusion sent provider satisfaction surveys to approximately 613,000 patients, and then publicly posted identifying and sensitive health information gleaned from the surveys. The FTC charged Practice Fusion with a series of deceptive business practices, including misrepresenting to patients that their survey responses would be communicated to the patients' providers, and failing to disclose that the survey responses would be published online. The terms of the proposed settlement place strict limits on Practice Fusion's business practices going forward, including prohibiting the company from misrepresenting the extent to which it uses, maintains, and protects the privacy and confidentiality of such sensitive information.

Read more about the case in our recent client alert.

MACRA Proposed Rule Changes the Medicare Payment Landscape

On April 27, 2016, the Centers for Medicare & Medicaid Services (CMS) released the Medicare Access and CHIP Reauthorization Act (MACRA) Notice of Proposed Rulemaking. The proposed rule made a series of important changes regarding how CMS pays Medicare providers. Specifically, it:

1. Ended the Sustainable Growth Rate (SGR) Formula.
2. Created the Quality Payment Program, which is now comprised of: (1) the new Merit-Based Incentive Payment System (MIPS), and (2) the new Alternative Payment Models (APMs) framework.

The new payment structures outlined in the proposed rule are designed to incentivize providers to deliver high-value rather than high-volume care to patients, while also streamlining the performance measurement process. The proposed rule establishes a new value-based scoring regime, piecing together elements of old performance measures with a series of new ones. Read more about MACRA and MIPS in our recent client alert.

Comments on the MACRA proposed rule are due on June 27, 2016 by 5:00 p.m.

The Push for Health IT Safety: The Precision Medicine Initiative and the New Data Security Framework

On May 25, 2016, the White House unveiled a new framework of privacy rules to protect health data collected as part of President Barack Obama's Precision Medicine Initiative (PMI). The PMI – a program aimed at fostering new tools, technologies, and therapies for disease prevention and treatment based on individualized patient health factors – launched on January 20, 2015, with an initial $215 million investment from the President's 2016 Budget. Of those funds, $5 million were dedicated to the Office of the National Coordinator for Health IT (ONC) to develop interoperability standards and requirements to protect patient privacy and ensure that data is securely exchanged across various systems. To continue and expand the PMI, the President's 2017 Budget pledges $309 million, with $5 million dedicated to ONC.

The new White House framework is based upon the National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, and emphasizes five key security functions:

1. **Identify** – Focuses on planning and security testing for PMI organizations. This function requires PMI organizations to: (1) develop a comprehensive security plan; (2) use risk-management strategies, tools, and techniques to make decisions about the best way to protect PMI data; (3) enlist independent third-party review of their security plans and plan effectiveness on a periodic basis; and (4) publicly post a high-level overview of the PMI organization's security plan to encourage greater transparency.
2. **Protect** – Focuses on ensuring that multiple layers of defense exist to safeguard PMI data, from the system level to the human level. PMI organizations must establish: (1) access controls; (2) security awareness and ongoing training; (3) data security; and (4) information protection and system maintenance operations.
3. **Detect** – Focuses on ensuring that there are continuous processes to detect security breaches and other data irregularities. PMI organizations must: (1) track and capture the "interactions" with PMI data by networks, servers, and users; (2) maintain uninterrupted audit logs; (3) create continuous detection and alert processes; (4) participate in threat information sharing forums and follow existing best-practices for users, as well as non-affiliated individuals, to report threats to the system; and (5) report security anomalies, alerts, and other relevant events.
4. **Respond** – Focuses on the actions that a PMI organization must take when things go wrong. Under this function, PMI organizations must have an incident response plan in place to quickly respond to and contain security incidents, and must regularly test that plan. If a security breach does occur, the organization must have a process in place to notify affected individuals and appropriate organizations in compliance with proper laws, the PMI Privacy and Trust Principles, and consistent with the organization's security plan. A PMI organization must also have an accountable point-person who will coordinate the incident response process.
5. **Recover** – Focuses on the aftermath of a security incident and the relevant take-aways: how do PMI organizations effectively learn from a breach? Under this function, organizations must already have an incident and breach recovery plan in place. PMI organizations must communicate with stakeholders, as well as identify and report "lessons learned" to its governance board and (as appropriate) other members of the PMI community.

The framework is not meant to prevent the release of appropriate non-identifiable, non-individualized information (*i.e*., aggregate research data, research findings, and information about ongoing research studies). In addition, although PMI organizations are free to create independent security plans based on a series of overarching Data Security Policy Principles listed at the beginning of the framework, PMI organizations can also use the more structured framework outlined above.

The framework was developed based on input from and collaboration between the Office of Science and Technology Policy; National Security Council; U.S. Digital Service; National Institute for Standards and Technology; Federal Trade Commission; Department of Veterans Affairs; Department of Defense; and Department of Health and Human Services, including its Office for Civil Rights, Office of the National Coordinator for Health IT, National Institutes of Health, Food and Drug Administration, and Centers for Medicare and Medicaid Services.

New White House Report Analyzes the Relationship Between "Big Data" and Civil Rights

In May, the White House released a report analyzing the intersection between "big data" and civil rights. Third in a series of publications by President Obama's Big Data Working Group, the report challenges the assumption that data is neutral by citing case studies on college admissions, criminal justice, employment, and credit lending which reveal that algorithms designed to turn data into information can harbor the biases of the people creating them. This is an important consideration for the health care sector. As health care organizations use big data for population health management and to measure and pay for health outcomes, it is important that new digital health technologies don't lead to greater health disparities or disparities in access to care.

The report serves as the catalyst for an ongoing discussion regarding the convergence of data and ethics. As part of that conversation, the National Science Foundation (NSF) has been directed to begin developing standards and techniques for the ethical collection and use of big data. The NSF has also been tasked with creating methods to teach these techniques to government agencies and businesses that increasingly rely on big data to drive strategic decisions.

FDA Releases Guidance on the Use of EHR Data in Clinical Trials

On May 17, 2016, the U.S. Food and Drug Administration (FDA) released draft guidance to facilitate the use of electronic health record (EHR) data for prospective clinical investigations of human drugs and biological products, medical devices, and combination products. The guidance is also intended to promote interoperability of EHRs that support clinical investigations.

The FDA states that widespread use of EHRs provides opportunities to improve patient safety, data accuracy, and clinical trial efficiency when data from these systems are used in clinical investigations.

The guidance includes recommendations on:

- Deciding whether and how to use EHRs as a source of data in clinical investigations.
- Using EHRs that are interoperable with electronic systems supporting clinical investigations.
- Ensuring the quality and the integrity of EHR data that are collected and used as electronic source data in clinical investigations.
- Ensuring that the use of EHR data collected and used as electronic source data in clinical investigations meets FDA's inspection, recordkeeping, and record retention requirements.

There is a preference shown for certified EHR technology – that is, EHRs certified under the Office of the National Coordinator for Health IT (ONC) Health IT Certification Program. However, non-certified EHRs can be used provided that adequate controls are in place to ensure the confidentiality, integrity, and reliability of data.

This guidance is designed to assist sponsors, clinical investigators, contract research organizations, institutional review boards (IRBs), and other interested parties on the use of EHR data in FDA-regulated clinical investigations.

The guidance builds on the following prior guidance:

- *Computerized Systems Used in Clinical Investigations*
- *Electronic Source Data in Clinical Investigations*

Comments are due July 18, 2016.

Patients to Receive Increased Access to Their Medical Device Data Under Proposed Guidance

On June 10, 2016, the U.S. Food and Drug Administration (FDA) released draft guidance to help increase patient access to their own medical device data. The draft guidance clarifies that medical device manufacturers are allowed to share patient-specific information that is recorded, stored, processed, retrieved, and/or derived from a medical device with the patient who is either treated or diagnosed with that specific device. The ultimate goal is to increase patient involvement in their own health care decisions.

The draft guidance provides specific considerations for manufacturers when communicating information to the patients regarding their own medical devices. Manufacturers should:

1. Consider the **content of the information**, including whether patients are able to easily interpret and understand the information they receive. The object is to prevent patient confusion, and avoid providing information that might be misinterpreted.
2. Ensure that the information is **comprehensive and up-to-date** so that patients have their full medical history, as well as their most recent medical information.
3. Provide **relevant context** to ensure that the information is not misinterpreted, including explaining certain background information or the circumstances of measurement to avoid misunderstandings.
4. Provide patients with **follow-up points of contact**, such as their health care provider or even the medical device manufacturer, so that the patient can ask questions as necessary.

The draft guidance not only reflects the FDA's general adherence to Health Insurance Portability and Accountability Act (HIPAA) principles; it also reflects broader government-wide goals to expand the right of individuals to access their own health information. Earlier this year, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released similar comprehensive guidance on the "right to access" issue. The FDA's draft guidance makes clear that its goals are aligned with OCR's: empowering patients to be more engaged in their health care, in hopes of achieving better health care outcomes.

Read more about patient access to medical device data on our blog here.

Health IT Resources Continue to Flow into Rural Communities

In their dedication to improving patient care outcomes, various federal agencies have continued to infuse health IT resources into underserved rural communities. The Medicare Access and CHIP Reauthorization Act (MACRA) proposed rule, released on April 27, 2016, gives the Centers for Medicare & Medicaid Services (CMS) $100 million to provide technical assistance to small and rural practices. The proposed rule allocates $20 million a year over five years to provide technical assistance via Quality Improvement Organizations (QIOs) and Regional Extension Centers (RECs) to practices with 15 or fewer eligible professionals participating in an Advanced Alternative Payment Model (APM) or the Merit-based Incentive Payment System (MIPS). Priority will be given to practices in rural and medically-underserved areas, as well as areas where there are a shortage of health professionals. This assistance is intended to position practices to transition to APMs or to improve MIPS composite scores.

On May 25, 2016, the Federal Communications Commission (FCC) released a Report and Order and Further Notice of Proposed Rulemaking related to its Connect America Fund (CAF), a subsidy-based effort to incentivize private wireline and wireless carriers to expand broadband support into remote and underserved communities. The May 25 Order includes general guidelines for CAF's Phase II competitive bidding process. (More specific details for the bidding process will be provided in the forthcoming Auction Procedures Public Notice.) The Order adds requirements for successful CAF Phase II bids, including: (1) four technology-neutral service standards for increased bidder flexibility; (2) a $215 million annual budget; (3) network build-out requirements, with specific coverage and service area benchmarks that must be met over a six-year period; (4) an application process for bidders; (5) reporting requirements; and (6) a framework for a Remote Areas Fund auction for areas that receive no winning bids in the CAF competitive bidding process.

Not surprisingly, according to a recent study in the Journal of the American Medical Informatics Association, "households with difficulty maintaining internet connectivity experienced significantly lower rates of internet health information seeking, reflecting the persistence of communication inequalities." The FCC's additional pledged support could have significant impacts on alleviating these health care barriers, not only for rural hospitals and other facilities, but for patient engagement as well. The FCC also continues to engage its Connect2HealthFCC initiative, including the Rural Health Care Program, to address the ongoing issues that exist at the intersection of broadband, advanced technology, and health care.

Comments on the MACRA proposed rule are due on June 27, 2016 by 5:00 p.m. Comments on the FCC Order are due 30 days after publication in the Federal Register.

Information Blocking: Congressional Reports, MACRA Attestation Requirements, and Public Pledges

Information blocking – knowing and unreasonable interference with the exchange or use of electronic health information – has received significant focus in recent months. Although information blocking has been a concern since early 2014, Congress catapulted the issue to the forefront of the health IT landscape on December 21, 2014 when it raised concerns about the practice. In response, the Office of the National Coordinator for Health IT (ONC) drafted a report to Congress on the issue in April 2015. The report addresses three key areas: (1) criteria to identify information blocking and distinguish it from other interoperability barriers; (2) an analysis of the nature and extent of information blocking, based on available evidence and industry knowledge; and (3) strategies and proposed solutions to address information blocking.

The recent release of the Medicare Access and CHIP Reauthorization Act (MACRA) proposed rule on April 27, 2016 has driven home the government's scrutiny of information blocking actions. Under the proposed rule, Merit-Based Incentive Payment System (MIPS) eligible clinicians and eligible professionals (EPs), eligible hospitals, and critical access hospitals under the EHR Incentive Program would be required to make attestations that they did not engage in information blocking. This is significant because if providers make attestations as part of MIPS or the Meaningful Use Program, and then act inconsistently with the attestations, they could be held in violation of the False Claims Act.

Since the Congressional call to action and ONC's responsive report, provider groups, technology companies, health IT organizations, and electronic health record (EHR) vendors have also made public pledges not to engage in information blocking. Signing such a public pledge, however, is not without its own risks: signatories could open themselves up to more Federal Trade Commission (FTC) scrutiny. According to a May 12, 2016 keynote address by FTC Chairwoman Edith Ramirez, the FTC has increased its "monitoring" of competition in the EHR space, including scrutinizing signs that dominant health care providers are using the lack of compatibility among EHR systems to deter patients from switching to other providers.

Read more about information blocking on our blog.

Advances in Telemedicine: Federal Quality Payment and State Parity

Medicare is still underspending on telemedicine initiatives, and state-level telemedicine "parity" laws have created more barriers than solutions. As a result, in recent months, lawmakers have taken steps to do something about these issues. At the federal level, the proposed CONNECT for Health Act would create incentives and opportunities for providers to incorporate telemedicine into their practices, as well as expand Medicare payments for telemedicine. For example, the proposed law would waive limitations on what qualifies as an "originating site" under Medicare; waive any geographic limitations (subject to state licensing requirements); waive any limitation on the use of store-and-forward technologies; and waive any limitation on the type of health care provider who may furnish such services (as long as the provider is a Medicare enrolled provider). The bill would also allow Medicare to cover remote patient monitoring services for individuals with certain chronic health conditions.

Under the Medicare Access and CHIP Reauthorization Act (MACRA) proposed rule, released on April 27, 2016, Medicare officials also hope to use the new Merit-Based Incentive Payment System (MIPS) and the proposed MIPS clinical practice improvement activities (CPIAs) category to encourage the use of telemedicine. These measures include using telehealth services and data analysis for quality improvement, such as participation in remote specialty care consultations.

In addition to proposed changes at the federal level, efforts to transform the landscape of telemedicine are also occurring at the state level:

- **Alaska**: On June 14, 2016, Governor Bill Walker signed H.B. 234 into law, which allows private insurance parity of telemental health services. In addition, S.B. 74 will remove the in-state presence requirements for prescribing via telemedicine, and authorizes the use of technology in certain clinical practices, including licensed audiologists, speech language pathologists, counselors, marriage and family therapists, psychologists, social workers, physical therapists, and occupational therapists. The Governor signed this bill into law on June 21, 2016.
- **Arizona**: On May 17, 2016, Governor Doug Ducey signed S.B. 1363 into law, requiring health plans to pay for telemedicine across the entire state beginning in 2018. The prior version of the state's parity law only required health plans to pay for telemedicine in rural and medically underserved areas.
- **Connecticut**: On June 7, 2016, Governor Dannel Malloy signed S.B. 298 into law, which requires the state to pay for telemedicine services through Medicaid.
- **Hawaii**: Lawmakers passed S.B. 2395, which allows parity coverage and reimbursement under Medicaid fee-for-service (FFS) and managed care. The bill also requires that telehealth encompass store-and-forward technologies, remote

monitoring, live consultation, and mobile health. It likewise ensures that telehealth is covered when originating in a patient's home and other non-medical environments. The bill is currently awaiting signature by Governor David Ige.

- **Kentucky**: On April 13, 2016, Governor Matt Bevin signed H.B. 95, which will allow its Medicaid program to cover home telemonitoring services and direct-to-patient telehealth services.
- **Louisiana**: Governor John Bel Edwards signed H.B. 480 into law on May 26, 2016, which allows physicians to prescribe controlled substances via telemedicine. H.B. 570, which would repeal the requirement that a physician practicing telemedicine maintain an office within the state, is currently awaiting the Governor's signature.
- **Missouri**: On June 8, 2016, Governor Jay Nixon signed a series of health-related bills, including S.B. 621 (combined as part of S.B. 579), which would expand Medicaid coverage to include store-and-forward, home remote patient monitoring, and other eligible sites and distant providers. The bill would also allow any state-licensed provider to use telehealth.

The flurry of activity at the federal and state levels is a sign of the rapidly-changing telehealth landscape. The federal government is creating the necessary reimbursement structures to encourage telemedicine development. Likewise, state governments are clearing the way for telemedicine reimbursement, easing telemedicine restrictions, and creating structures to support better patient access and patient-centered approaches that are necessary to improve long-term health outcomes. With such rapid development and change, more telemedicine advances are sure to be on the horizon.

Funding Opportunities: ONC HIP Cooperative Agreement Program and the SEA Cooperative Agreement Program

On May 9, 2016, the Office of the National Coordinator for Health IT (ONC) announced the High Impact Pilots (HIP) Awards program, pledging $1.25 million to the development of health IT. The cooperative agreement program is designed to spur the implementation of standards and technology to improve interoperability, improve health care delivery, and demonstrate how health IT can positively impact patient experiences. Funds will be divided among three to seven awardees, each receiving between $100,000 and $500,000. Letters of intent were due on June 10, 2016. The deadline for applications is July 8, 2016.

For their projects, HIP awardees will select a "Priority Category," and then select at least three "Impact Dimensions":

Priority Categories and Subcategories:

1. **Comprehensive Medication Management** (subcategories: Drug Cost at Care; Opioid)
2. **Care Coordination** (subcategories: Care Plan; Closed-Loop Referral)
3. **Labs** (subcategory: Full-Loop Laps)
4. **Self-Identified**

Impact Dimensions:

1. Practice Efficiency
2. **Safety**

3. **Privacy & Security**
4. **Clinical Quality**
5. **Patient Experience**
6. **Cost Efficiency**
7. **Interoperable Exchange**

On May 9, 2016, ONC also announced the Standards Exploration Awards (SEA) program. The SEA program – also a cooperative agreement program – is identical to the HIP program, except on a smaller scale. The SEA program will make three to five awards of $50,000 to $100,000 each, and SEA awardees need only select one Impact Dimension compared to HIP's three. Applicants may apply for both the HIP and the SEA programs, but must submit separate applications for each program. The deadline for applications is also July 8, 2016.

For both programs, awardees must use and incorporate the best available standards, implementation guides, and emerging alternatives identified in the 2016 Interoperability Standards Advisory (ISA). With a 12-month performance period, awardees will also have a fairly tight turn-around. However, both programs seem promising as catalysts for one of the most important parts of health IT development: measurable, field-tested experiential data.

Questions about both programs can be directed to ONC.techlab@hhs.gov. Slides from the May 23, 2016 HIP Information Session are available here, and slides from the May 26, 2016 SEA information session are available here.

Funding Opportunity: Move Health Data Forward Challenge

On May 10, 2016, as part of the America COMPETES Reauthorization Act of 2010, the Office of the National Coordinator for Health IT (ONC) launched the Move Health Data Forward Challenge. The Challenge will award $250,000 to participants whose technical projects allow patients to securely authorize and control the movement of their health data. The Challenge incentivizes participants – including health IT developers, health care providers, and other entities with relevant expertise – to create an application programming interface (API) solution (Solution) that meets privacy and security specifications established by the HEART Workgroup (an alliance of security, privacy, and health IT stakeholders tasked with developing specifications for the electronic exchange and use of health information).

The Challenge itself will have three Phases:

1. **Phase 1 – Proposals**: Awards up to 10 finalists with $5,000 each based on submitted proposals. Participants will be required to describe the technical, operational, financial, and business aspects of their proposed Solution. Phase 1 participants will be judged on: (1) Participant Capabilities; (2) Impact Potential; and (3) Executability. Phase 1 winners will be eligible to move on to Phase 2.
2. **Phase 2 – Prototype and Pilot**: Awards up to five finalists with $20,000 each based on the prototype of their Solution. Participants must demonstrate the effectiveness of the Solution and its impact on accessibility and data exchange of patient health records by the patients themselves or by providers. The focus will be on potential value and successful

outcomes in improving the quality of health care. Phase 2 participants will be judged on: (1) Technical Merit; (2) Viability; and (3) Impact. Phase 2 winners will be eligible to move on to Phase 3.

3. **Phase 3 – Scale and Implement**: Awards up to two winners with $50,000 each based on their ability to implement their respective Solutions. This phase will require participants to test their Solution in "real-life" situations. Participants must demonstrate a consumer-facing Solution that incorporates the privacy and security specifications developed by the HEART Workgroup. Phase 3 participants will be judged on: (1) Impact; (2) Deployability; and (3) Scalability.

Challenge participants can apply independently or as part of a team. Phase 1 Challenge submissions are due on September 8, 2016. Submissions will be evaluated from September 9 to October 14, 2016, and Phase 1 winners will be announced on October 31, 2016.

More information about the Challenge is also available on ONC's website here.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com