crowell moring

CLIENT ALERT

Digital Health – Recent Developments

March 2016

In this alert:

President Obama Addresses Precision Medicine, Health IT, Data Access, and Security

A year ago the president launched the Precision Medicine Initiative (PMI) to accelerate medicine that delivers the right treatment at the right time, taking into account individuals' health history, genes, environments, and lifestyles. On February 25, President Obama addressed a small audience at the White House, identifying the need for patient participation in health care and the importance of individualizing treatments for a particular patient. Obama said precision medicine can lead to reduced costs, better care, and a more efficient health care system. This includes efforts by the NIH to build a one million-person voluntary national research cohort who will partner with researchers, share data, and engage in research to transform our understanding of health and disease through precision medicine.

Many announcements were made. A contract was awarded to Vanderbilt in collaboration with Verily to launch the research cohort. NIH and ONC announced "Sync for Science" pilots through an open standards development process, with six electronic health record developers, to help scale individual data access and donation for precision medicine research. FDA launched a precision FDA challenge, which will encourage the genomics community to advance quality standards and achieve more consistent and accurate DNA test results.

Read more on our blog.

Funding Opportunities

Medicaid Matching Funds Available to Connect Providers Eligible for Meaningful Use with other Providers

There is a very significant funding opportunity for State Medicaid Programs, which can support use of health information technology by health care providers that provide care to Medicaid recipients and those who may exchange information with Medicaid providers eligible for Meaningful Use incentives. It may also benefit technology developers that are engaged in health information exchange efforts.

On February 29, CMS released a letter to State Medicaid Directors expanding the scope of available federal funding at the 90 percent matching rate under the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 for state expenditures on activities to promote health information exchange (HIE) and encourage the adoption of certified Electronic Health Record (EHR) technology by certain Medicaid providers. This can provide significant financial resources for providers who are not eligible for the CMS EHR Incentive Program (the "Meaningful Use Program"). CMS states that they will look favorably on collaborative efforts that support interoperability.

Read more on our blog.

Challenge Grants for Health Apps

The Office of the National Coordinator for Health IT (ONC) announced two software app challenges with award prizes totaling $175,000 each:

- Consumer Health Data Aggregator Challenge: To spur the development of third-party, consumer-facing applications that use open, standardized APIs to help consumers aggregate their data in one place and under their control.
- Provider User Experience Challenge: For the development of applications that use open, standardized APIs to enable innovative ways for providers to interact with patient health data. This challenge will focus on demonstrating how data made accessible to apps through APIs can positively impact providers' experience with EHRs by making clinical workflows more intuitive, specific to clinical specialty, and actionable.

The challenge has two phases. Phase 1 requires the submission of technical and business plans for the application by May 30, 2016. Phase 2 requires the development of the apps, verification of technical capabilities, user testing/piloting, and public release of the apps. It will conclude on November 7 (in time for the presidential election).

Additionally, a competitive funding opportunity of up to $275,000 will support the development of an open resource to make it easier for developers to publish their apps and for providers to discover and compare them. The strategy will leverage the HL-7 Fast Healthcare Interoperability Resources (FHIR) standard and the use of open, standardized application programming interfaces (APIs).

Public Comment Periods

The ONC Proposes the Direct Review of Certified Health IT in Oversight Rule

On March 1, the Office of the National Coordinator for Health Information Technology (ONC) announced the Enhanced Oversight and Accountability Rule (the Oversight Rule), a proposed rule that would change the ONC Health IT Certification Program (certification program). The Oversight Rule would expand ONC's role in the certification program. Specifically, the Oversight Rule would provide ONC with express powers to directly review health IT certified under the certification program and employ review, suspension, and termination processes to address "non-conformities" found in certified health IT. The ONC is seeking comment on key issues such as the scope of ONC's proposed direct review authority, its processes for reviewing certified and uncertified health IT capabilities, and the agency's potential overlap with the authority of other agencies. **All public comments will be due to ONC on or before May 1, 2016**. Crowell & Moring would be happy to help prepare comments. For more information, see our blog.

Precision Medicine Security Principles

On February 25, 2016, the Precision Medicine Initiative released a draft *Data Security Policy Principles and Framework* for public comment. Building from the existing PMI Privacy and Trust Principles, this document offers security policy principles and a framework to guide decision-making by organizations conducting or participating in precision medicine activities. **This document is open for public comments and will be finalized later this spring.**

Update the Model Privacy Notice

The Office of the National Coordinator for Health IT (ONC) announced that it is updating the Model Privacy Notice (MPN) that was developed to provide a standardized, easy-to-use framework for developers to clearly convey information about privacy and security to their users and for consumers to be able to compare these policies across products. The MPN is a voluntary tool that was developed originally for use by developers of personal health records and was modeled after the FDA nutrition facts label. Now, there are significantly more types of consumer health technologies, many of which are not covered by HIPAA, and

different uses of data. ONC is looking to update the MPN and published a Request for Information to obtain comments on the scope and content of the MPN. Specifically, they are requesting input on information practices health technology developers should disclose to consumers and what language should be used to describe those practices in an updated MPN. **Comments are due on April 15, 2016**. This is an opportunity to give feedback to the federal government on the scope and content. I am personally excited about the update to this as the creator of the original MPN.

Regulations and Guidance

CMS Extends Deadline for Meaningful Use Hardship Exemption

The CMS has extended the deadline, to July 1, 2016, for eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) to file applications for "hardship" exemptions from the meaningful use requirements of the EHR incentive payment program for 2015. They have streamlined the hardship application process to reduce the amount of information that must be submitted as a result of changes under the Patient Access and Medicare Protection Act (PAMPA), which established that the Secretary may consider hardship exceptions for "categories" of EPs, eligible hospitals, and CAHs. Successfully applying for the hardship exception will prevent payment adjustments in 2017.

HHS Releases HIPAA/NIST Crosswalk

The U.S. Department of Health and Human Services (HHS) released a "crosswalk" or "mapping" document which identifies commonalities between the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF) and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. HIPAA covered entities must implement data security safeguards to comply with the HIPAA Security Rule. HHS's new crosswalk is designed to help health care organizations that use the CSF to identify gaps in their security programs, help address those gaps, and map their HIPAA compliance measures to the industry standards identified in the CSF.

HHS Publishes PHI Access Fees FAQs

HHS provided a set of FAQs on appropriate fees for the release of Personal Health Information (PHI) to patients. The FAQs come second in a series of guidance that HHS has provided to help covered entities (e.g., health plans and health care providers) understand a patient's HIPAA Right of Access to his or her own PHI, and the proper methods for releasing that information directly to the patient or a third-party at the patient's request. The guidance will help health care providers and health plans understand when and how they can provide patient access to records within the confines of the HIPAA Privacy Rule, and how they may recoup the cost of providing that access. This guidance comes in response to many concerns about high charges to patients for access to their records that may be beyond what is permitted by HIPAA.

HHS Releases PHI Disclosure Fact Sheets

In order to clear up misconceptions about Health Insurance Portability and Accountability Act (HIPAA) limitations on disclosing Protected Health Information (PHI), in February, HHS Office of the National Coordinator for Health Information Technology (ONC) released a series of new fact sheets and guidance, including guidance regarding common situations (treatment and health care operations). The series includes: 1) The Real HIPAA Supports Interoperability; 2) Permitted Uses and Disclosures; 3) Care Coordination, Care Planning, and Case Management Examples; and 4) Quality Assessment/Quality Improvement and Population-Based Activities Examples. These documents are intended to provide clarity, but do not set new HIPAA policy.

HHS Guidance on Health Apps and HIPAA

The U.S. Department of Health and Human Services (HHS) provided use scenarios to aid health app developers to determine whether their activities and apps are subject to the rules of the Health Information Portability and Accountability Act (HIPAA). HIPAA requires covered entities (e.g., health plans and health care providers) to comply with the HIPAA rules and business associates (e.g., those creating or offering apps on behalf of a covered entity or other business associate) to comply with certain HIPAA rules. The guidance released by HHS will help app developers with the threshold determination of whether they are subject to HIPAA. HHS has said it intends to provide more guidance to the public.

California AG Defines "Reasonable Security"

The California Attorney General published the 2016 "California Data Breach Report," which lays out what the state believes to be "reasonable security" for the purpose of California's law that requires protecting personal information. This is the first time California has recommended an external industry standard as a baseline "reasonable security" requirement. According to the California AG, the chosen standard (Center for Internet Security's (CIS) Critical Security Controls (formerly known as the SANS Top 20)) is a consensus list of the "best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks," and is updated periodically to keep up with technology. The FTC has previously recommended using industry standards, but did not go as far as California in prescribing a particular one. Given California's size and prominence as an active enforcer of privacy and security laws, and the fact that its privacy law applies to most businesses that collect personal information on California residents, these recommendations essentially create a set of baseline requirements for many companies.

EU-US Privacy Shield Principles Released

After years of negotiations that intensified after the U.S.-EU Safe Harbor program was invalidated late last year, the U.S. Department of Commerce (DOC) and the European Commission (EC) reached an agreement to replace Safe Harbor, called the

EU-U.S. Privacy Shield. On February 29, the DOC formally published this agreement. The EC also published the draft adequacy decision for the new framework. This formal agreement largely tracks the priorities discussed in a press release issued earlier in February and will allow companies to plan for lawful data transmissions across the Atlantic.

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