HHS Opens Up National Patient Access to Lab Test Reports

Save to myBoK

By AHIMA's Advocacy and Policy Team

The healthcare patient engagement revolution rolls on in the US, with the latest victory for patient advocates coming via a change in patient access rights to lab test information. New legislation recently enacted makes it easier than ever before for all US patients to gain access to their medical laboratory results and records.

On February 6, 2013, the Centers for Medicare and Medicaid Services (CMS) published the final rule "Clinical Laboratory Improvement Act (CLIA) Program and Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule; Patients' Access to Test Reports." This final rule amends the CLIA amendments of 1988 "to specify that, upon request of a patient (or the patient's personal representative), laboratories subject to CLIA may provide the patient, the patient's personal representative, or a person designated by the patient, as applicable, with copies of completed test reports that, using the laboratory's authentication process, can be identified as belonging to the patient." Further, the final rule amends the HIPAA Privacy Rule so that individuals and/or their personal representatives can access their test reports directly from CLIA-covered labs. The final rule is effective on April 7, 2014, and requires compliance by HIPAA-covered entities by October 6, 2014.

Law Standardizes a National Right to Access Labs

In a continued effort to increase access to personal health information, CMS worked with the Office of the National Coordinator for Health IT (ONC), the Centers for Disease Control and Prevention (CDC), and the Department of Health and Human Services' Office for Civil Rights (OCR) to implement the records rights change. Prior to this final rule, the existing rules regarding access to lab results were identified as a barrier to the exchange of health information and a barrier to patient access and participation in their own care by ONC's Health Information Technology Policy Committee. The HIPAA Privacy Rule originally had exceptions for CLIA, but this final rule removes those exceptions so that individuals can have direct access to all test reports from CLIA-certified laboratories.

Ultimately the rule impacts labs in two ways:

- Establishes new individual access provisions
- Requires labs to revise their HIPAA Privacy Rule requirements

The impact of this final rule will vary between states and territories. There are 16 states and territories where it will have little or no impact because they already permit patient access to test results (Delaware, Washington, DC, Maryland, New Hampshire, New Jersey, Nevada, Oregon, Puerto Rico, and West Virginia) or permit access with provider approval (California, Connecticut, Florida, Massachusetts, Michigan, New York, and Virginia). Those states and laboratories that do not already permit access would have to develop access mechanisms. The final rule indicates that there are 22,816 laboratories impacted by the new access provisions.

With regard to revising the HIPAA Notice of Privacy Practices, the rule identifies the laboratories in Delaware, Washington, DC, Maryland, New Hampshire, New Jersey, Nevada, Oregon, Puerto Rico, and Virginia as not needing to revise their notices. The labs in the remaining states and Guam, the Northern Mariana Islands, and the Virgin Islands will need to revise their notices due to the preemption of their state laws.

NIST Releases Cybersecurity Framework

All too often recently the media has reported on stories of hackers gaining access to personal information—such as the data breaches at retailer Target, the University of Maryland, the *New York Times*, and major social media sites such as Facebook and Twitter. With every hack comes a different element of danger, whether it is financial information, health information,

national security, or even political protesting. To help combat this growing problem President Obama issued Executive Order 13636 on February 12, 2013.

The order directed the Executive Branch to:

- Develop a technology-neutral voluntary cybersecurity framework
- Promote and incentivize the adoption of cybersecurity practices
- Increase the volume, timeliness, and quality of cyber threat information sharing
- Incorporate strong privacy and civil liberty protections into every initiative to secure the US' critical infrastructure
- Explore the use of existing regulation to promote cybersecurity

Through a February 26, 2013 request for information (RFI), a series of workshops and a public comment period, the National Institute of Standards and Technology (NIST) developed and issued the Cybersecurity Framework on February 12, 2014. The Cybersecurity Framework "consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[1]

NIST has also developed the "NIST Roadmap for Improving Critical Infrastructure Cybersecurity." The roadmap focuses on several important directives strengthening private sector involvement in future governance of the framework. Areas for development, alignment, and collaboration include authentication; automated indicator sharing; conformity assessment; growing the cybersecurity workforce; data analytics; federal agency cybersecurity alignment; international aspects, impacts, and alignment; supply chain risk management; and technical privacy standards.

NIST will continue to develop the Cybersecurity Framework and welcomes additional informal feedback on the framework and the accompanying roadmap. Comments or thoughts on this work can be sent to NIST at cyberframework@nist.gov.

Congress Finds Permanent Fix to SGR

After years of annually fixing the sustainable growth rate (SGR) formula, Congress has seemingly struck a bipartisan agreement that will permanently replace the problematic physician payment formula that was first included in the 1997 budget agreement. Since 2003, Congress' annual fix to the physician Medicare payment rates has cost taxpayers over $150 billion. The most recent patch expired March 31, 2014.

The chairs and ranking members of committees in the US Senate and House introduced their specific bills on February 6, 2013. Former Senate Finance Committee Chairman Max Baucus (D-MT) and ranking member Orrin Hatch (R-UT) introduced S. 2000, the "SGR Repeal and Medicare Provider Payment Modernization Act." In the House, identical legislation, HR 4015, was introduced by House Ways and Means Committee Chairman Dave Camp (R-MI), House Ways and Means Committee Ranking Member Sander Levin (D-MI), House Energy and Commerce Committee Chairman Fred Upton (R-MI), and House Energy and Commerce Committee Ranking Member Henry A. Waxman (D-CA). The formal intent of S. 2000 and HR 4015 is to "amend title XVIII of the Social Security Act to repeal the Medicare sustainable growth rate and improve Medicare payments for physicians and other professionals, and for other purposes."

Congress has struggled to find a solution to this annual issue. This year, the Senate Finance Committee, the House Ways and Means Committee, and the House Energy and Commerce Committee were determined to reach a bipartisan agreement, and have done so. According to the summary, the bill would:

- Repeal the SGR and end the annual threat to seniors' care, while instituting a 0.5 percent payment update for five years.
- Improve the fee-for-service system by streamlining Medicare's existing web of quality programs into one value-based performance program, which increases payment accuracy and encourages physicians to adopt proven practices.
- Incentivize movement to alternative payment models to encourage doctors and providers to focus more on coordination and prevention to improve quality and reduce costs.
- Make Medicare more transparent by giving patients more access to information and supplying doctors with data they can use to improve care.

The SGR revamp proposal also impacts the "meaningful use" EHR Incentive Program by placing it into a robust incentive program called the Merit-Based Incentive Payment System (MIPS). MIPS includes the Physician Quality Reporting System

(PQRS), the Value-Based Payment Modifier, and meaningful use, effectively making Medicare a pay-for-performance system rather than a volume-based/fee-for-service payment system.

Note

1. National Institute of Standards and Technology. "Cybersecurity Framework." Federal Register 79, no. 32 (February 18, 2014): 9167.

The AHIMA Advocacy and Policy Team (advocacyandpolicy@ahima.org) is based in Washington, DC.

Article citation:
AHIMA Advocacy and Policy Team. "HHS Opens Up National Patient Access to Lab Test Reports" *Journal of AHIMA* 85, no.4 (April 2014): 16-17.