Oversight of Government Privacy, Security Rules for Health Data Questioned

July 16, 2012

Oversight and accountability for following federal privacy and security rules is critical if the public is going to trust that the next generation of electronic health care providers, insurers, and billing services can protect the privacy of their medical information. A recent report [1] by the Government Accountability Office questions whether sufficient work is being done to build that public trust.

The GAO report says the Department of Health and Human Services has failed to issue new rules for protecting personal health information and lacks a long-term plan for ensuring that those new rules are being followed. The HHS Office for Civil Rights (OCR), which is responsible for overseeing these efforts, acknowledged these concerns but noted that rules are winding their way through government channels and that they have "taken the necessary first steps towards establishing a sustainable" oversight program.

The report's two main concerns are: (1) the urgent need for guidance on de-identification methods, and (2) lack of a long-term plan for auditing covered entities and business associates for compliance with federal privacy and security rules (specifically, HIPAA [2] and HITECH [3]).

De-Identification Guidance

De-identification is a tool that enables health data to be used for a broad range of purposes while minimizing the risks to individual privacy. Under HIPAA, there are two methods that can be used to de-identify health data. The first is the safe harbor method [4], which merely requires the removal of 18 specific categories of identifiers, such as name, address, dates of birth or health care services, and other unique identifiers. The second is the expert determination method that certifies that the data, in the hands of the intended recipient, raises a very small risk of re-identification. The safe harbor method is static and presumes that the removal of the 18 categories of identifiers translates into very low risk of re-identification in all circumstances.

In HITECH, Congress directed HHS to complete a study of the HIPAA de-identification standard by February 2010. Though covered entities rely more on the safe harbor method because it is easier to understand and more accessible, OCR aimed to produce guidance that would "clarify guidelines for conducting the expert determination method of de-identification to reduce entities reliance on the Safe Harbor method," according to the report. Two years later and notwithstanding its good intentions, OCR has not released this guidance.

CDT has met with industry and consumer stakeholders about how to improve federal policy regarding de-identified health data since 2009. CDT also recently published [5] an article in JAMIA proposing a number of policies to strengthen HIPAA de-identification standards and ensure accountability for unauthorized re-identification.

The OCR should issue the required guidance on de-identification without further delay and continue seeking public feedback on how to build trust in uses of de-identified data. Foot dragging on this issue risks impeding progress on the ability to monitor the public's health in ways that go far beyond [6]mere notification and routine reporting of symptoms, diagnoses, etc. With these new capabilities in place, public health officials can move beyond traditional detection and response to outbreaks, enabling earlier disease detection, allowing public health officials to take a more active role monitoring health issues from cancer screening to adult immunizations to HIV.

Ensuring Compliance

Routine audits help ensure that covered entities and business associates comply with HIPAA and HITECH regulations. Audits also provide OCR with important information about how entities covered

by HIPAA and HITECH are implementing critically important privacy and security protections, and potentially surface issues needing further regulatory guidance and helping OCR better determine when penalties for noncompliance are warranted.

HITECH directed HHS to audit entities [1] covered by HIPAA for compliance with HIPAA and new HITECH requirements; OCR officials began those audits [1] earlier this year. The report states that OCR has no plan to sustain these audits beyond 2012; the report also notes that HHS does not have a defined plan for including HIPAA business associates in its audits. HHS responded that OCR plans to review the pilot audit program at the end of this year and move forward with an audit program after that step is complete.

If the public is to trust that the privacy of their health information is well protected, it must know where that information is going and how it's being used. The report highlights the importance of audits as an effective mechanism for accountability. CDT is encouraged by the progress OCR has made to date in its pilot audit program, and we are pleased to see HHS commit to learning from the pilots to developing and implementing a sustained plan for auditing compliance with federal privacy and security regulations.

-
- HITECH
- hipaa
- Health Privacy

The content throughout this website that originates with CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. Details.
Copyright © 2013 by Center for Democracy & Technology.

Source URL:
https://cdt.org/blogs/suchismita-pahi/1607oversight-government-privacy-security-rules-health-data-questioned

Links:
[1] http://www.gao.gov/assets/600/591807.pdf
[2] http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf
[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
[5] http://jamia.bmj.com/content/early/2012/06/25/amiajnl-2012-000936.full
[6] http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2528028/