Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: GAO Calls on HHS to Tighten Cybersecurity Guidance, Oversight

Report highlights the security issues that threaten federal electronic health information.

A new report (link here: http://www.gao.gov/assets/680/679260.pdf) from the Government Accountability Office (GAO) is calling on the HHS to beef up its security guidance and oversight when it comes to protecting electronic health information.

Background. In 2015 alone, 113 million EHRs were breached a significant bump from the 12.5 million EHRs breached the year before. In 2009, that number was less than 135,000 (not a typo). In addition, the number of reported breaches affecting records of at least 500 individuals rose from zero in 2009 to 56 last year, almost double from 2014.

GAO input. According to the GAO, while the HHS is responsible for establishing standards for protecting electronic health information and for enforcing compliance, the agency's security and privacy guidance doesn't fully address important elements outlined in current federal cybersecurity guidance. The GAO found that the health agency's oversight actions don't always check that existing rules have even been implemented.

Ease and Convenience Beget Responsibility

EHRs can make it easier for providers to share information and give patients ready access to their health information, among other benefits. However, EHR systems are vulnerable to cyber-based threats that can jeopardize the confidentiality, integrity, and availability of the information they contain. Data breaches experienced by covered entities and their business associates have resulted in millions of individuals having sensitive information compromised.

Take a look at this. For example, in July 2014, Community Health Services said hackers took records, including Social Security numbers, patient names, birth dates, addresses and telephone numbers, belonging to some 4.5 million people, and that's not an isolated incident. In May 2015, UCLA reported that hackers stole a trove of data that included "personally identifiable information (PII) such as names, addresses, dates of birth, Social Security numbers, medical record numbers, Medicare or health plan ID numbers, and some medical information."

"Criminals are aware that obtaining complete health records are often more useful than isolated financial information, such as credit information," the GAO said in the report. "Electronic health records often contain extensive amounts of information about an individual."

Federal advice. To help curb threats like this, the HHS established guidance for covered entities such as health plans and care providers in complying with HIPAA's requirements for ensuring the privacy and security of Protected Health Information (PHI). However, according to the GAO, this guidance doesn't address important controls included in other federal cybersecurity guidance.

For instance, as required by HIPAA, the HHS issued the security, breach notification, and privacy rules, as amended by the HITECH Act, and has implemented an oversight program to enforce compliance by covered entities and business associates. However, the HHS guidance does not address how covered entities should tailor their implementations of key security controls identified by the National Institute of Standards and Technology (NIST) to their specific needs, and so may not be as effective as it could be.

The OCR Gets Involved

Although HHS's Office for Civil Rights (OCR) continues to close thousands of cases per year, the closure activities in a significant number of cases do not provide assurance that identified issues have been addressed.

But, sometimes there's a lack of direction from the OCR. When technical assistance is used to close cases, the OCR doesn't always address the complaint directly or provide meaningful direction to organizations on how to comply with the security and privacy rules. In addition, cases that are closed with incomplete corrective actions and no follow-up do not provide assurance that covered entities and their business associates are completing the actions as agreed, according to the GAO.

Improvements on the way. The OCR has reported on steps it is taking to improve privacy and security in the healthcare sector, including taking significant enforcement actions and implementing its audit program. But, according to the GAO, without establishing measures for progress in improving security and privacy through its audit program, it'll be difficult to determine whether the program is effective.

Additionally, the GAO found that the OCR does not routinely coordinate with CMS to help ensure that only eligible entities receive Meaningful Use (MU) incentive payments under the HITECH Act's EHR program.

The GAO Recommends that HHS Take Action

In its research, the GAO found certain things lacking in the HHS cybersecurity dealings, and as a result, advised the governmental agency to take action. Here is a list of the top five recommendations the GAO put forth to help HHS address its shortcomings:

1. Update security guidance for covered entities and business associates to ensure that the guidance addresses implementation of controls described in the NIST Cybersecurity Framework;
2. Update technical assistance that is provided to covered entities and business associates to address technical security concerns;
3. Revise the current enforcement program to include following up on the implementation of corrective actions;
4. Establish performance measures for the OCR audit program; and
5. Establish and implement policies and procedures for sharing the results of investigations and audits between the OCR and CMS to help ensure that covered entities and business associates are in compliance with HIPAA and the HITECH Act.

Here's The HHS Response

HHS agreed with three of the five recommendations (numbers 1, 2, and 4) and said it would take actions to implement them. It also promised to mull over the remaining two recommendations (numbers 3 and 5).

Number three. Regarding the third recommendation that the HHS revise the current enforcement program to include following up on the implementation of corrective actions the agency said that for settlement agreements, the OCR already follows up with healthcare entities to ensure corrective actions have been taken.

While the GAO agreed that for these cases, follow-up does indeed occur, it suggested that for cases that don't result in a settlement agreement, ensuring that the corrective actions have been taken into account would provide greater assurance that entities have implemented HIPAA compliance actions.

The lowdown on five. The agency noted that the OCR already shares information with CMS on breach reports. But, the GAO insists that the OCR doesn't yet share information about the results of its investigations with CMS.

"However, for some of its investigations it provided technical assistance that was not pertinent to identified problems, and in other cases it did not always follow up to ensure that agreed-upon corrective actions were taken once investigative cases were closed," the GAO said. "Further, the office has not yet established benchmarks to assess the effectiveness of its audit program."

Endnote. Sharing this information, according to the GAO, could allow CMS to ensure that recipients of financial incentives under the HITECH Act's MU program have met the requirements for those incentives.