Margaret Reetz Partner
margaret.reetz@mendes.com
Mendes & Mount LLP, New York

Image: Jared Arango / Unsplash.com

Members of Congress chase the HHS for answers on healthcare sector cyber security oversight

In a letter addressed to the US Department of Health and Human Services ('HHS') Secretary, Alex Azar, Congressional committee chairmen and ranking members outlined how the HHS response to implementation of the Cybersecurity Information Sharing Act of 2015 ('CISA')[1] has been lacking and inconsistent ('the Letter'). In this article Margaret Reetz, Partner at Mendes & Mount LLP, discusses the concerns raised in the letter and the likely actions of the HHS.

Congress insisted on a two week turnaround after the Letter was issued, which ended up in hearings before certain subcommittees, in closed session. Healthcare entities and insurers have been prominent targets for cyber attacks for many years, given the wealth of information stored and managed by these entities. The HHS, therefore, has a unique and significant role in trying to ensure the integrity of these information systems and it appears that US Congress, on a rare bi-partisan basis, remembered it had a role in exerting some influence over the HHS in this area.

Information sharing to information security

Even a casual observer is cognizant that a healthcare provider, a treatment centre or a health insurer has an extraordinary charge in safeguarding information within its control[2]. In the US, healthcare data breaches top the lists of the most significant and expensive attacks[3]. For these reasons, Congress and the Obama administration identified the healthcare sector as a leading focus for proposed private and public partnerships to identify cyber security threats and harden defenses against attacks on information systems.

On 18 December 2015, President Obama signed into law the Cybersecurity Information Sharing Act of 2015 ('CISA'), under which the HHS is required to submit a 'Cyber Threat Preparedness Report' ('CTPR') as well as provide a status update 'regarding the alignment of 'Health Care Industry Security approaches' (as noted in the Letter). Not without controversy at the time of its enactment[4], CISA established mechanisms by which: (i) federal departments and agencies were to share cyber security information with one another and with non-federal entities; and (ii) non-federal entities were to share cyber security information with one another and with federal departments and agencies[5]. CISA provided 'safe harbors' for private entities that shared such information, in accordance with the procedures and processes to be outlined by the Department of Homeland Security ('DHS'). Despite ominous alarm bells sounded by civil liberties groups in a post-NSA surveillance scandal landscape[6], sharing data with the Government was on a voluntary basis and required federal authorities and organisations to first 'remove personal information, or information that identifies a specific person' pre-sharing[7].

Apart from the headline-grabbing 'sharing' proposal, CISA also directed the HHS to develop cyber security best practices for organisations in the healthcare industry, under Section 405 of Title IV of CISA. That provision states that the HHS secretary is to establish and regularly update these standards. The standards are to be consistent with the Heath Insurance Portability and Accountability Act of 1996 ('HIPAA') Security Rule, and the secretary was to create a public-private task force to review how to secure networked medical devices and other software or systems connected to electronic health records[8]. Following these directives, the HHS launched a Health Cybersecurity and Communications Integration Center ('HCCIC')[9]. However, notwithstanding an initial flourish of pronouncements and advisories[10], apparently key personnel at the HHS became the subjects of internal investigations and were reassigned, and ultimately reportedly left their original positions or the HHS altogether[11]. Thus, it appears Congress started to take notice and has since pursued the HHS Secretary for a more robust status update and specifics regarding the department's accountability with respect to cyber threats.

Questions from Congress

In the Letter dated 5 June 2018, members from the Energy and Commerce Committee and the Health, Education, Labor and Pensions Committee recounted how the HHS delivered its CTPR on 27 April 2017 to Congress[12]. The CTPR was intended

continued

to clarify the HHS's internal roles, responsibilities, and preparedness to address threats to the healthcare sector, according to the Letter. The Letter notes, however, that the CTPR "omitted or lacked sufficient detail on many outstanding issues," like the HHS's dual role in providing support to stakeholders following an incident or attack, while continuing with its obligations as a regulatory enforcement agency *vis-à-vis* these same stakeholders. The Letter also criticised the HHS for creating a policy gap in failing to specify which of the HHS' operating divisions or offices is to respond in the event of an incident (incidents involving electronic health records and/or medical devices, for example, which potentially would necessitate involvement of another federal agency, the Food and Drug Administration).

The supposed launch of the HCCIC was also criticised, with the Letter stating that few details were provided and there was "little clarity on how the HCCIC would fit into the larger health care cybersecurity picture," raising concerns of duplication of effort by the DHS and others. The HHS did not even mention the HCCIC in its CTPR submitted as of May 2017, and as the Letter notes, the HHS credited the HCCIC with a smooth response to the WannaCry threats in 2017 but by September 2017 the HHS had reassigned two senior officials responsible for the day-to-day operations of the HCCIC. Attention was drawn to "stakeholders" reporting that "they no longer understand whether the HCCIC still exists, who is running it, or what capabilities and responsibilities it has[13]." The Letter cautions that these problems "have exacerbated the very issues that CISA was intended to address."

It was also noted that the HHS was required to establish a "collaborative process" with Government officials and health care industry stakeholders. The Letter states "as of this writing, HHS still has not produced the 'common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes' required by the law[14]." As such, it was suggested that the HHS take certain actions, including: providing an update to the CTPR (any updates to cyber security strategies); provide a detailed explanation of the HCCIC (how it intersects with the NCCIC, etc.); address internal HHS coordination; address the role of the HHS in securing its own systems; and, address any challenges the HHS faces as both a regulator and oversight agency. Finally, the Letter set a deadline for the HHS to respond to these questions and suggestions.

According to news reports and statements by the committees, while the HHS response has not been published, a subcommittee to the House Energy and Commerce Committee heard testimony as of 20 June regarding Governmental Accountability Office audits of the HHS cyber security programs. Reportedly, the discussion had to be held in closed session due to the "sensitive" nature of the issues discussed and "to protect information that may endanger national security[15]."

Actions to be taken

In a statement as part of an earlier hearing before the Committee on Energy and Commerce Subcommittee on Health, the Chief Security and Privacy Officer for the University of Chicago Medicine and a co-chair for a CISA task group commented that "[m]any healthcare providers are under-resourced and need assistance navigating [the] new [cyber security] threat environment[16]. While praising the response post-WannaCry, the task group co-chair commented that its "members cite confusion about who leads HHS' cybersecurity programs and the correct way to communicate with the Department concerning cybersecurity-related issues." He also noted the concerns regarding how to share information to an entity charged with an enforcement function. The task group suggested that in order to "enhance proactive collaboration, there should be incentives to industry, such as monetary subsidies or safe harbors from enforcement actions." The task group asked that the HHS offer "flexibility" in its enforcement actions, where providers: 1) demonstrate adoption of the National Institute of Standards and Technology ('NIST') Cybersecurity Framework; and 2) adopt the relevant best practices being delivered through the CSA 2015 405(d) Task Group.

In his testimony, Erik Decker, the CISO and task group co-chair analogised the attention to and handling of these threats to how clinicians have standard hygiene practices of washing their hands or how agencies and stakeholders provide large scale emergency responses to worldwide disease outbreaks, like ebola and the zika virus. Another suggestion was to move the HCCIC from the HHS's Office of the Chief Information Officer to its Office of the Assistant Secretary for Preparedness and Response ('ASPR'), which deals with public health emergencies. One significant concern would be whether that office had the relevant technical expertise to address cyber security issues[17].

Likely outcomes

Given the framework set up for the HCCIC, despite some initial personnel issues and apparent internal in-fighting, it would appear somewhat more likely that the HHS will try to emphasise its ability and agility to respond to cyber security threats by working through the current structure instead of a wholesale reorganisation. It could be that the HHS is a victim of its own success in pursuing and highlighting entities that have been the victims of cyber attacks but also may have been lax in their own security practices, exposing patients and consumers to threats. Even while some questioned whether the HHS would be stepping on the toes of the DHS with its significant cyber security role, others were hopeful at the time of its launch that thr HCCIC would be more sensitive to the challenges faced by providers and more responsive in sharing information concerning threats[18].

Meanwhile, over at the DHS, the NCCIC may be the beneficiary of any proposals for funding to strengthen the government's ability to identify and respond to threats. One funding proposal addresses industrial control systems[19]. The healthcare industry will certainly take note of the comparisons to threats involving industrial control systems and threats to medical devices and their attendant systems and controls. These are more often than not mentioned in the same discussion by cyber security professionals[20]. It remains to be seen whether the HHS will be eclipsed or get swept along by its DHS counterparts.

Image: Nathan Dumlao / Unsplash.com

The Letter took aim at the supposed launch of the HCCIC, stating that few details were provided and there was "little clarity on how the HCCIC would fit into the larger health care cybersecurity picture," raising concerns of duplication of effort by the DHS and others.

1. Consolidated Appropriations Act, 2016, Pub. L. 114-113, 129 STAT. 2981-2984, 18 Dec. 2015.
2. See a discussion regarding use of data brokers and comments regarding survey respondents reporting "they would hide information from their doctors if it was shared through an Electronic Health Record (EHR), and [...] would withhold information or postpone seeking care if they had a sensitive medical condition." http://chicagopolicyreview.org/2015/11/19/hidden-threats-to-healthcare-data-privacy-outside-of-hipaa-protections/
3. "Heavily regulated industries, including healthcare, experienced higher data breach costs." https://healthitsecurity.com/news/healthcare-data-breach-costs-highest-for-7th-straight-year (citing research from the 2017 Ponemon Cost of Data Breach Study.
4. "The controversial 'surveillance' act Obama just signed, E. Rosenfeld, CNBC, 22 Dec 2015, updated 2:50 pm EST; https://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html
5. CISA was signed into law on 18 December 2015, as Division N of the Consolidated Appropriations Act of 2016. See discussion of history leading up to passage of bill. A Quick Guide to the Senate's Newly Passed Cybersecurity Bill, L. Greenemeier, 28 October 2015, Scientific American; https://www.scientificamerican.com/article/a-quick-guide-to-the-senate-s-newly-passed-cybersecurity-bill/
6. The 'Shadow Brokers' continued to release details of the U.S. National Security Agency's reported "hacking tools" as of 2017. https://www.cbsnews.com/news/new-leak-suggests-nsa-penetrated-banking-networks-in-the-middle-east/ Originally leaked with the help of a former intelligence contractor, Edward Snowden, as of 2013, details of the breadth of NSA's reported surveillance efforts endure as a cause for activists and a concern for governmental agencies. https://www.washingtonpost.com/news/wonk/wp/2016/04/27/new-study-snowdens-disclosures-about-nsa-spying-had-a-scary-effect-on-free-speech/?noredirect=on&utm_term=.5278d9a9aa35
7. Privacy and security professionals worried that only a 'cursory review' of indicators would take place, not entirely ensuring complete de-identifying. https://www.healthcareitnews.com/blog/apple-vs-fbi-and-cybersecurity-act-2015-3-questions-ask-sharing-data#gs.E6HHakQ
8. The HIPAA Security Rule requires safeguards with respect to electronic protected health information ('ePHI'). https://www.hhs.gov/hipaa/for-professionals/security/index.html The task force was to report on ways to improve preparedness and responses to threats. https://iapp.org/news/a/key-u-s-cybersecurity-provisions-signed-into-law/
9. The HCCIC reportedly launched as of Spring 2017 and was to be modeled after the DHS' National Cybersecurity and Communications Integration Center ('NCCIC'). https://searchhealthit.techtarget.com/blog/Health-IT-Pulse/HHS-announces-launch-of-new-cybersecurity-center; soon after their announcement, HHS officials took credit for communication efforts to thwart any 'WannaCry' threats in 2017. http://www.modernhealthcare.com/article/20170608/NEWS/170609910
10. The HHS officials claimed to be shifting the sector from 'compliance' footing to 'a dynamic risk approach;' Congress still wondered whether the efforts would reach small practices and rural hospitals. https://www.healthdatamanagement.com/news/hhs-center-for-cyber-threat-sharing-helped-lead-response-to-malware-attack
11. 'HHS cybersecurity initiative paralyzed by ethics, contracting investigation,' D. Tahir, 13 November 2017, posted at 5:44pm EST; https://www.politico.com/story/2017/11/13/hhs-cybersecurity-initiative-paralyzed-by-ethics-contracting-investigation-244855
12. A complete copy of the Letter is at: http://energycommerce.house.gov/wp-content/uploads/2018/06/20180605HHS.pdf
13. See the Letter, page 3; "WannaCry is a ransomware worm that spread rapidly through across a number of computer networks in May of 2017." J. Fruhlinger, CSO Online, 27 September 2017, posted at 2:37am, PST; https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html
14. See the Letter at page 4.
15. Public Opening Statement of Chairman Gregg Harper; https://docs.house.gov/meetings/IF/IF02/20180620/108445/HHRG-115-IF02-MState-H001045-20180620.pdf
16. Testimony before the United States House of Representatives Committee on Energy and Commerce Subcommittee on Health, 6 June 2018, statement of Erik Decker; https://docs.house.gov/meetings/IF/IF14/20180606/108389/HHRG-115-IF14-Wstate-DeckerE-20180606.pdf
17. 'Cyber drama on Hill today,' D. Tahir, 6 June 2018, posted at 10:00am EDT, Politico; https://www.politico.com/newsletters/morning-ehealth/2018/06/06/cyber-drama-on-hill-today-243470
18. 'HHS' Cyber Info Sharing Center: Is It Needed?' M. McGee, 27 June 2017, HealthcareInfoSecurity; https://www.careersinfosecurity.com/hhs-cyber-info-sharing-center-needed-a-10038
19. See, H.R. 5733, the DHS Industrial Control Systems Capabilities Enhancement Act of 2018; https://policy.house.gov/legislative/bills/hr-5733-dhs-industrial-control-systems-capabilities-enhancement-act-2018
20. Siemens and the DHS issue advisories regarding medical device vulnerabilities. 'DHS, Siemens Warn of Potential Medical Device,' E. Snell, HealthITSecurity, 7 August 2017; Vulnerabilitieshttps://healthitsecurity.com/news/dhs-siemens-warn-of-potential-medical-device-vulnerabilities