HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Aug 28, 2025

This week, Health-ISAC®'s Hacking Healthcare® examines evidence that the HIPAA Security Rule effort launched at the end of the Biden administration may be moving ahead under the Trump administration, and that the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) might miss its October deadline by more than a few months.

Welcome back to Hacking Healthcare®.

Evidence Suggests New Dates for HIPAA Security Rule and Cyber Incident Reporting

U.S. presidential administration transitions often begin with months of policy reviews and reversals as the new administration rushes to enact its own policy vision. The first months of the second Trump administration have been no different, but they have thrown two important cybersecurity efforts into question. While there has been very little official news on the progress of the HIPAA Security Rule Proposed Rule that the Biden administration published in early January, or the long running effort by the Cybersecurity and Infrastructure Security Agency (CISA) to complete the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Final Rule, we may now have some evidence about what to expect and when.

HIPAA Security Rule Recap

As many are aware, over the past few years, there has been significant support for updating the HIPAA Security Rule to account for changes in technology and the cyber threat landscape. That support materialized in the last weeks of the Biden administration as the Department of Health and Human Services (HHS) published a fairly substantial proposed Rule.

However, the change in presidential administration in January, which included a lengthy pause and review of Biden-era policies, cast doubt on the fate of the proposed update. HHS under the Trump administration has not been vocal about what it plans to do with the HIPAA Security Rule, leaving uncertainty over whether it might continue with the Biden era proposal with minimal modifications, heavily revise it to better align with Trump administration goals, or put it on indefinite hold since there is no legal obligation to update the Rule.

New Evidence of Ongoing Efforts

At the time of writing, HHS has not publicly commented on the status of its HIPAA Security Rule effort. However, new evidence suggests there are still plans to move forward with it.

So where does this evidence come from?

Within the Office of Management and Budget (OMB), there is the Office of Information and Regulatory Affairs (OIRA), and within the General Services Administration (GSA) is the Regulatory Information Service Center (RISC). These two offices coordinate to publish the Unified Agenda of Federal Regulatory and Deregulatory Actions ("Unified Agenda"). This agenda "provides uniform reporting of data on regulatory and deregulatory activities under development throughout the Federal Government, covering approximately 60 departments, agencies, and commissions."[i] Generally included in the agenda are activities that are "currently planned to have an Advance Notice of Proposed Rulemaking (ANPRM), a Notice of Proposed Rulemaking (NPRM), or a Final Rule issued within the next 12 months."[ii]

The agenda is generally compiled and published twice a year, once in the Spring and once in the Fall. While the Trump administration did not publish a Spring update, two weeks ago, an update briefly appeared on the Unified Agenda webpage that looked to be the expected Fall 2025 update. However, the update was quickly taken down, and the Unified Agenda webpage reverted to the prior Fall 2024 version. Before that reversal could be completed, Bloomberg Law reportedly noticed and took screen captures of the apparent Fall 2025 Unified Agenda.[iii] These captures included what appear to be updates to the existing HIPAA Security Rule and the CIRCIA agenda entries.

While Unified Agenda entries are fairly basic in terms of content, Bloomberg's screen captures suggest that HHS is targeting a HIPAA Security Rule Final Rule around May of next year, and CISA will miss the October CIRCIA deadline, pushing it to mid-2026 as well.[iv]

To be absolutely clear, while this "leak" is compelling, we urge members to be prudent in assessing its veracity, and no one should confuse this with an official confirmation of policy decisions by either HHS or CISA. Under the assumption that it is accurate, let's dig into what to make of this new evidence in the Action & Analysis portion of this week's Hacking Healthcare.

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.reginfo.gov/public/jsp/eAgenda/UA_About.myjsp
[ii] https://www.reginfo.gov/public/jsp/eAgenda/UA_About.myjsp
[iii] https://www.bloomberglaw.com/product/blaw/bloomberglawnews/bloomberg-law-news/BNA%2000000197-d175-db96-a3ff-ff7f40730000
[iv] https://www.bloomberglaw.com/product/blaw/bloomberglawnews/bloomberg-law-news/BNA%2000000197-d175-db96-a3ff-ff7f40730000
[v] https://www.regulations.gov/docket/HHS-OCR-2024-0020/comments
[vi] https://www.reginfo.gov/public/jsp/eAgenda/UA_About.myjsp

Reference(s)	reginfo, reginfo 1, bloomberglaw, bloomberglaw 1, regulations, reginfo 2
Report Source(s)	Health-ISAC

Alert ID 123b819c

View Alert

Share Feedback
was this helpful? | |

Tags Cyber Incident Reporting for Critical Infrastructure, Cyber Incident Reporting, Security Rule, CIRCIA, Hacking Healthcare, CISA, HHS, HIPAA

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits

https://h-isac.org/events/

Hacking Healthcare

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**