

Hacking Healthcare - Weekly Blog

Hacking Healthcare

TLP:WHITE

Alert Id: df056c40

2024-11-26 13:04:36

This week, Health-ISAC®'s Hacking Healthcare® takes an initial look at what we may expect from the incoming Trump administration. In particular, we address how a change in administration may impact development of ongoing rules and regulations, the likelihood of new federal healthcare cybersecurity laws, the organization and resourcing of relevant federal agencies, and broad international policy alignment.

Welcome back to Hacking Healthcare®.

A First Look at Healthcare Cybersecurity Under a Trump Administration

It is too early to make accurate predictions on who may lead specific health care and cybersecurity initiatives or what kinds of issues might be prioritized under the Trump administration. However, based on past actions and current political rhetoric, some high-level themes can be drawn. This iteration of Hacking Healthcare will explore some of them and analyze why they may or may not come to fruition.

Action & Analysis

Included with Health-ISAC Membership

Conclusion

As we stated at the beginning, there is a lot of uncertainty over how all of this will play out, in part due to the likelihood of infighting, novel legal and policy approaches, and unintended second-order effects. We will strive to provide a more in-depth analysis in the new year when the dust settles on congressional appointments, agency leads, and public policy outlines.

^[i] For those looking for a refresher, we would encourage you to read Hacking Healthcare from July 18 on how Chevron may impact the healthcare sector. <https://health-isac.org/health-isac-hacking-healthcare-7-18-2024/>

^[ii] CISA was given 18 months from the publication of the draft proposed rulemaking to publish the final rulemaking.

^[iii] [https://clayhiggins.house.gov/2024/11/19/higgins-introduces-legislation-improving-cybersecurity-protections/#:~:text=%E2%80%93%20Congressman%20Clay%20Higgins%20\(R%2D,combating%20the%20threat%20of%20cyberattacks.](https://clayhiggins.house.gov/2024/11/19/higgins-introduces-legislation-improving-cybersecurity-protections/#:~:text=%E2%80%93%20Congressman%20Clay%20Higgins%20(R%2D,combating%20the%20threat%20of%20cyberattacks.)

^[iv] <https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf>

^[v] https://www.finance.senate.gov/imo/media/doc/health_infrastructure_security_and_accountability_act_one-pager.pdf

^[vi] <https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf>

^[vii] <https://health-isac.org/health-isac-hacking-healthcare-7-18-2024/>

Reference(s): [cisa](#), [HHS](#), [house](#), [health-isac](#), [senate](#)

Report Source(s): Health-ISAC

Release Date: Nov 27, 2024 (UTC)

Tags: Regulatory, CIRCA, Hacking Healthcare, White House, Trump administration, HIPAA, European Union, United States

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.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" [here](#).

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" [here](#).

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