SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare ○ TLP:WHITE Alert ID : 68e18068 Dec 01, 2023, 08:20 AM

This week, *Hacking Healthcare™* examines newly proposed cybersecurity regulations for hospitals in New York State. We begin by breaking down what we expect to see from the publicly unreleased draft language before shifting our focus to analyzing the potential impact, troubling provisions, and expected next steps.

Welcome back to *Hacking Healthcare*™.

New York State Proposes New Hospital Cybersecurity Regulations

On November 13th, New York State Governor Kathy Hochul's office published a press release announcing proposed cybersecurity regulations for New York State hospitals designed to "safeguard health care systems from growing cyber threats."[i] Governor Hochul has described the proposed regulations as a "nation-leading blueprint" that are meant to complement existing Health Insurance Portability and Accountability Act (HIPAA) provisions. Let's take a look at what is being proposed and how it may impact healthcare sector entities.

While the full proposal is not yet public, at a mid-November meeting of New York State's Public Health and Health Planning Council, Matt Wiley, the Emergency Preparedness Manager in the Office of Primary Care and Health Systems Management for the New York State Department of Health, gave a brief overview of the proposed regulations.[ii] His comments, combined with the Governor's initial press release, give us some idea as to what to expect from the proposed regulations that would add a new section, 405.46, to Title 10 of the New York Codes, Rules and Regulations.

The proposed hospital cybersecurity regulations are expected to include the following:[iii], [iv]

- Hospitals will need to report cybersecurity incidents affecting operations within a two-hour time frame.

- The proposed regulations will define key terms and create distinctions between cybersecurity events and cybersecurity incidents, and they will also address confidentiality and the applicability of state and federal statutes.

- Hospitals will be required to establish a comprehensive program covering risk assessment, response, recovery, and data protection.

- Hospitals will need to create specific cybersecurity policies, including asset management, access, control, training, monitoring, and incident response.

- Hospitals will need to conduct regular cybersecurity testing, including scans and penetration testing.

- The proposed set of regulations "defines qualifications and skills for cybersecurity staff"

- The proposed regulations will set policies for third-party cybersecurity providers.

- Hospitals will be required to run tests of their response plan to ensure that patient care continues while systems are restored back to normal operations.

- Hospital cybersecurity programs will need to include written procedures, guidelines, and standards to develop secure practices for in-house applications intended for use by the facility.

- Hospitals will also be required to establish policies and procedures for evaluating, assessing, and testing the security of externally developed applications used by the hospital.

- Hospitals will need to establish a Chief Information Security Officer (CISO) role, if one does not exist already, in order to enforce the new policies and to annually review and update them as needed.

- Hospitals will need to require the use of multi-factor authentication (MFA) to access the hospital's internal networks from an external network.

- Proposed regulations will have a 1-year grace period for compliance from the date of adoption, however, the reporting requirements would be immediate upon adoption.

Let's break down what some of these provisions will mean for affected entities, put the regulation in context with existing and potential federal policy, and outline what comes next.

Action & Analysis
Included with Health-ISAC Membership

[i] https://www.governor.ny.gov/news/governor-hochul-announces-proposed-cybersecurity-regulations-hospitals-throughout-new-york#:~:text=Under%20the%20proposed%20provisions%2C%20hospitals,access%20or%20other%20malicious%20acts%2C
[ii] https://totalwebcasting.com/view/?func=VIEW&id=nysdoh&date=2023-11-16&seq=1
[iii] https://www.governor.ny.gov/news/governor-hochul-announces-proposed-cybersecurity-regulations-hospitals-throughout-new-york#:~:text=Under%20the%20proposed%20provisions%2C%20hospitals,access%20or%20other%20malicious%20acts%2C
[iv] https://totalwebcasting.com/view/?func=VIEW&id=nysdoh&date=2023-11-16&seq=1
[v] https://totalwebcasting.com/view/?func=VIEW&id=nysdoh&date=2023-11-16&seq=1

Report Source(s)

Health-ISAC

Reference | References

totalwebcasting
Attorney General

Tags

Legislation, Regulatory, Hacking Healthcare, New York State, New York, cybersecurity

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

For Questions and/or Comments:

Please email us at contact@h-isac.org

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 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 Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org