Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : 1b943584 | Dec 15, 2022, 03:01 PM

This week, Hacking Healthcare begins by examining a new notice of proposed rulemaking by HHS that asks stakeholders to provide feedback on the implementation of part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The mental-health focused proposed rule touches on issues of security, privacy, and disclosure and is meant to bring better alignment with HIPAA requirements. Next, we breakdown a recent FBI appeal to health sector organizations as to why cyberattack victims should engage with the FBI. Regardless of whether you are convinced by the arguments, we outline one reason why you may want to reassess your reluctance.

Welcome Back to *Hacking Healthcare*.

HHS: New Proposed Rule Touches on Security, Privacy, and Disclosure

On December 2, the Department of Health and Human Services published a Notice of Proposed Rulemaking in the federal register that would modify its regulations to implement Section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[i] While the proposed rule appears fairly targeted in scope, its effects may be more outsized than they appear at an initial glance.

The proposed rule relates to "to the Confidentiality of Substance Use Disorder (SUD) Patient Records under 42 CFR part 2 (Part 2), which protects patient privacy and records concerning treatment related to substance use challenges from unauthorized disclosures."[ii] The most significant changes may be those that create greater alignment between Part 2 and HIPAA's Privacy, Breach Notification, and Enforcement rules. HHS Secretary Becerra described the proposed rule as one that "would improve coordination of care for patients receiving treatment while strengthening critical privacy protections to help ensure individuals do not forego life-saving care due to concerns about records disclosure."[iii]

The Substance Abuse and Mental Health Services Administration (SAMHSA) within HHS summarized some of the major changes in a press release. Some of the more prominent security and privacy aspects addressed in the proposed rule include:[iv]

- Permitted redisclosure of Part 2 records, in any manner, permitted by the HIPAA Privacy Rule, with certain exceptions.
- New patient rights under Part 2 to obtain an accounting of disclosures and to request restrictions on certain disclosures, as also granted by the HIPAA Privacy Rule.
- Expanded prohibitions on the use and disclosure of Part 2 records in civil, criminal, administrative, and legislative proceedings.
- New HHS enforcement authority, including the imposition of civil money penalties for violations of Part 2.
- Updated breach notification requirements to HHS and affected patients.
- Updated HIPAA Privacy Rule Notice of Privacy Practices requirements to address uses and disclosures of Part 2 records and individual rights with respect to those records.

The proposed rule can be found on the Federal Register at: https://www.federalregister.gov/documents/2022/12/02/2022-25784/confidentiality-of-substance-use-disorder-sud-patient-records

Action & Analysis

Included with H-ISAC Membership

FBI Attempts to Assuage Healthcare Sector Fears Over Cyberattack Response Involvement

Earlier this week at the HIMSS Cybersecurity Forum, Special Agent Private Sector and Academic Coordinator for the FBI's Boston Division, Bill McDermott, made the case for reaching out to the FBI when organizations in the healthcare sector find themselves victimized by a cyberattack.[vi] While there is a certain level of skepticism that many in the private sector have about how helpful federal law enforcement can be, it may be time to reassess that stance given that mandatory incident reporting requirements are on the way.

After apparently opening with a joke about the terror and/or cynicism that some feel when they hear, "I'm from the government and I'm here to help," McDermott went on to try and disabuse some of the notions that private sector organizations have about the FBI that are mistaken.[vii] He made the case that while certain malware might be new to a victim, it is possible that the FBI has a freely available decryption key because it's something that they have already dealt with.

McDermott also addressed some of the more significant concerns that organizations have about how the FBI engages and what their follow-up actions are likely to be. McDermott was clear in disputing the notion that once they are contacted, a team of FBI agents bedecked in gear will suddenly show up at the victim organization's facilities or that the FBI will further harm victims by looking for additional violations once they get involved.

Even if you aren't convinced by an FBI agent's defense of his own organization, there is another reason for healthcare sector entities to reassess their perspective on FBI engagement.

Action & Analysis

Included with H-ISAC Membership

Congress

Tuesday, December 6th:

- No relevant hearings

Wednesday, December 7th:

- No relevant hearings

Thursday, December 8th:

- No relevant hearings

[i] https://www.federalregister.gov/documents/2022/12/02/2022-25784/confidentiality-of-substance-use-disorder-sud-patient-records
[ii] https://www.samhsa.gov/newsroom/press-announcements/20221128/hhs-increase-care-coordination-confidentiality-patients-substance-use-challenges
[iii] https://www.samhsa.gov/newsroom/press-announcements/20221128/hhs-increase-care-coordination-confidentiality-patients-substance-use-challenges
[iv] https://www.samhsa.gov/newsroom/press-announcements/20221128/hhs-increase-care-coordination-confidentiality-patients-substance-use-challenges
[v] https://www.nextgov.com/policy/2022/12/proposed-rule-would-prioritize-patient-consent-dealing-mental-health-data/380339/
[vi] https://www.healthcareitnews.com/news/fbi-special-agent-call-cyber-operations-center-when-attacks-occur
[vii] https://www.healthcareitnews.com/news/fbi-special-agent-call-cyber-operations-center-when-attacks-occur
[viii] https://www.healthcareitnews.com/news/fbi-prevents-nebraska-hospital-cyber-attack
[ix] https://www.healthcareitnews.com/news/boston-childrens-hospital-was-target-cyberattack-thwarted-fbi
[x] https://www.zdnet.com/article/cisa-pledges-to-share-incident-reports-with-fbi-after-doj-backlash/

Reference | References

ZDNet
Nextgov
Health-ISAC
Healthcare IT News
Healthcare IT News
samhsa
federalregister
Healthcare IT News

Report Source(s)

Health-ISAC

Tags

Incident Reporting, CIRCIA, Hacking Healthcare, CARES Act, FBI

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:

Written by John Banghart, who served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council's 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 Council's 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.
John can be reached at jbanghart@h-isac.org and jfbanghart@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.