Health-ISAC Weekly Blog -- Hacking Healthcare

Hacking Healthcare | TLP:WHITE | Alert ID : d05633e4 | Jun 01, 2023, 02:31 PM

This week, *Hacking Healthcare* takes a look at an upcoming Federal Trade Commission proposed rulemaking that would clarify and strengthen its Health Breach Notification Rule. We examine what the rule is, how it relates to the Health Insurance Portability and Accountability Act (HIPAA), and why it might matter to healthcare organizations not covered by it.

Welcome back to *Hacking Healthcare*.

Federal Trade Commission Proposes Revising Its Health Breach Notification Rule

The Federal Trade Commission (FTC) published a press release on May 18th to announce its intention to assess "amendments to strengthen and modernize the Health Breach Notification Rule (HBNR)."[i] While not a regulatory measure that directly affects those entities covered by HIPAA, the Rule has been drawing attention as a response to "health apps and other direct-to-consumer health technologies, such as fitness trackers, [having become] commonplace."[ii] The proposed Rule changes, and FTC Commissioner Rebecca Kelly Slaughter's recent comments on the Rule, raise questions about the increasing regulatory attention given to data privacy and protection of sensitive health data.

For those unfamiliar with the FTC's HBNR, it "requires vendors of personal health records ("PHRs") and related entities that are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") to notify individuals, the FTC, and in some cases, the media of a breach of unsecured personally identifiable health data."[iii] The Rule fits within the FTC's broader priorities to protect sensitive consumer data. While the Rule has been in force since 2010, it wasn't until this year that any enforcement actions were taken.

The notice of proposed rulemaking and request for comment come after a 2020 review of the Rule received widespread stakeholder support to "clarify that the Rule applies to apps and similar technologies" and for the FTC to "take additional steps to protect unsecured PHR identifiable health information that is not covered by HIPAA, both to prevent harm to consumers."[iv]

Additionally, stakeholders commented that the FTC should step up enforcement and that clarification would help "level the competitive playing field among companies dealing with the same health information."[v]

While the FTC did provide updated guidance along these lines in 2021, the agency appears ready to formalize changes to the HBNR.[vi] Those proposed changes seek to:

(1) clarify the Rule's scope, including its coverage of developers of many health applications ("apps");

(2) amend the definition of breach of security to clarify that a breach of security includes data security breaches and unauthorized disclosures;

(3) revise the definition of a PHR-related entity;

(4) clarify what it means for a vendor of personal health records to draw PHR identifiable health information from multiple sources;

(5) modernize the method of notice;

(6) expand the content of the notice; and

(7) improve the Rule's readability by clarifying cross-references and adding statutory citations, consolidating notice and timing requirements, and articulating the penalties for non-compliance.

The FTC is open to receiving public comments from interested stakeholders on these issues for 60 days once it has been formally published within the *Federal Register*, which has not taken place at the time of writing.

Action & Analysis
Included with Health-ISAC Membership

Recommendations

For those members directly affected by the FTC rule, there is likely value in reviewing the proposed changes and submitting comments on any issues you may have or any clarifications you may want. This may be the only formal opportunity to help shape future FTC action on this issue.

For members who are not as directly impacted by this rule, perhaps because you are covered by HIPAA, it's worth noting that there continues to be a legal and regulatory focus on the privacy and protection of health data. Furthermore, it may be interesting to see how some of the FTC's proposed changes to notification may be received.

While the FTC and the Department of Health and Human Services (HHS) do not have exactly the same goals, authority, or expertise, the FTC's openness to expanding the amount and type of information required in its HBNR notices signals a desire to better inform, educate, and provide relief to affected individuals for violations to their health data beyond what is expressly required by healthcare regulations like HIPAA. While HHS is under no obligation to follow the FTC's lead, and other differences and considerations are present that may preclude simply copying its approach, it may incentivize HHS to consider if this is an area worth updating. It may also spark interest in HHS to update HIPAA more broadly, which is long overdue and a subject we cover routinely here.

Conclusion

The FTC's publication of an RFC on this issue helps illustrate another avenue by which sensitive personal health-related data is permeating areas beyond traditional healthcare. Tangible regulatory efforts outside the HHS to better protect health data at large within the United States is broadly a good thing, but it does raise the issue of potential divergences between the kinds of privacy and security protections and incident notices that each regulator believes are appropriate. We don't yet know how many of these proposed changes will be pursued by the FTC, but it will be worth watching. It's also worth noting that the current administration is very interested in achieving regulatory harmonization, both within the United States and internationally. Whether the FTC is keeping this in mind is unclear, but is something we should all encourage it to consider.

Congress
Tuesday, May 30
No relevant hearings

Wednesday, May 31
No relevant meetings

Thursday, June 1
No relevant hearings

International Hearings/Meetings
No relevant meetings
EU

[i] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule
[ii] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule
[iii] https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_health_breach_notification_rule_nprm.pdf
[iv] https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_health_breach_notification_rule_nprm.pdf
[v] https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_health_breach_notification_rule_nprm.pdf
[vi]https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf
[vii] https://www.ftc.gov/system/files/ftc_gov/pdf/slaughter-ocm-oral-remark-5-18-2023.pdf

[viii] https://www.ftc.gov/system/files/ftc_gov/pdf/slaughter-ocm-oral-remark-5-18-2023.pdf
[ix] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[x] https://www.ftc.gov/system/files/ftc_gov/pdf/slaughter-ocm-oral-remark-5-18-2023.pdf
[xi] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[xii] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-318
[xiii] https://www.ftc.gov/system/files/ftc_gov/pdf/HBRN-NPRM-%28CLEAN%29-revised2.pdf
[xiv] https://www.ftc.gov/system/files/ftc_gov/pdf/HBRN-NPRM-%28CLEAN%29-revised2.pdf

Report Source(s)

Health-ISAC

Reference | References

ecfr
FTC
FTC
HHS
FTC
FTC
FTC

Tags

Hacking Healthcare, Breach Notification, FTC

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.