[Billing Code: 6750-01S]

FEDERAL TRADE COMMISSION

16 CFR Part 318

Health Breach Notification

AGENCY: Federal Trade Commission.

ACTION: Regulatory review; request for public comment.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") requests public comment on its Health Breach Notification Rule (the "HBN Rule" or the "Rule"). The Commission is soliciting comment as part of the FTC's systematic review of all current Commission regulations and guides.

DATES: Written comments must be received on or before [INSERT DATE 90 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file a comment online or on paper by following the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write "Health Breach Notification Rule, 16 CFR part 318, Project No. P205405," on your comment and file your comment online at https://www.regulations.gov by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex B), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Elisa Jillson (202-326-3001), Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION:

I. Background

The Commission typically reviews its rules every ten years to ensure that the rules have kept up with changes in the marketplace, technology, and business models.[1] The Commission issued the HBN Rule in 2009, and companies were subject to enforcement beginning in 2010. The Commission now requests comment on the HBN Rule, including the costs and benefits of the Rule, and whether particular sections should be retained, eliminated, or modified. All interested persons are hereby given notice of the opportunity to submit written data, views, and arguments concerning the Rule.

The HBN Rule, issued pursuant to section 13407 of the American Recovery and Reinvestment Act of 2009 ("Recovery Act" or "the Act"),[2] became effective on August 25, 2009,[3] and companies were subject to FTC enforcement beginning on February 22, 2010. Section 13407 of the Recovery Act created certain protections for "personal health records" or "PHRs," electronic records of identifiable health information that can be drawn from multiple sources and that are managed, shared, and controlled by or primarily for the individual. Specifically, the Recovery Act recognized that vendors of personal health records and PHR related entities (i.e., companies that offer products and services through PHR websites or access information in or send information to PHRs) were

[1] See current ten-year schedule for review of FTC rules and guides at 85 FR 20889 (Apr. 15, 2020).
[2] Public Law No. 111-5, 123 Stat. 115 (2009).
[3] 74 FR 42962 (Aug. 25, 2009).

collecting consumers' health information but were not subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act ("HIPAA").[4] The Recovery Act directed the FTC to issue a rule requiring these entities, and their third-party service providers, to provide notification of any breach of unsecured individually identifiable health information. Accordingly, the HBN Rule requires vendors of PHRs and PHR related entities to provide: (1) notice to consumers whose unsecured individually identifiable health information has been breached; (2) notice to the media, in many cases; and (3) notice to the Commission. The Rule also requires third party service providers (i.e., those companies that provide services such as billing or data storage) to vendors of PHRs and PHR related entities to provide notification to such vendors and entities following the discovery of a breach.

The Rule requires notice "without unreasonable delay and in no case later than 60 calendar days" after discovery of a data breach. If the breach affects 500 or more individuals, notice to the FTC must be provided "as soon as possible and in no case later than ten business days" after discovery of the breach. The FTC makes available a standard form for companies to use to notify the Commission of a breach.[5] The FTC posts a list of breaches involving 500 or more individuals on its website.[6] This list only includes two breaches, because the Commission has predominantly received notices about breaches affecting fewer than 500 individuals.

---

[4] Health Insurance Portability & Accountability Act, Public Law No. 104-191, 110 Stat. 1936 (1996).
[5] Notice of Breach of Health Information, *https://www.ftc.gov/system/files/documents/plain-language/2017_5_2_breach_notification_form.pdf*.
[6] Breach Notices Received by the FTC, *https://www.ftc.gov/system/files/documents/plain-language/draft_breach_notices_received_by_ftc_2015.pdf*.

Importantly, the Rule does not apply to health information secured through technologies specified by the Department of Health and Human Services ("HHS") and it does not apply to businesses or organizations covered by HIPAA. HIPAA-covered entities and their "business associates" must instead comply with HHS's breach notification rule.[7] The FTC has not had occasion to enforce its Rule because, as the PHR market has developed over the past decade, most PHR vendors, related entities, and service providers have been HIPAA-covered entities or "business associates" subject to HHS's rule.[8] However, as consumers turn towards direct-to-consumer technologies for health information and services (such as mobile health applications, virtual assistants, and platforms' health tools), more companies may be covered by the FTC's Rule.

II. Rule Review

The Commission periodically reviews all of its rules and guides. These reviews seek information about the costs and benefits of the Commission's rules and guides and their regulatory and economic impact. The information obtained assists the Commission in identifying those rules and guides that warrant modification. Therefore, the Commission solicits comments on, among other things, the economic impact and benefits of the Rule; possible conflict between the Rule and state, local, or other federal laws or regulations; and the effect on the Rule of any technological, economic, or other industry changes.

[7] HIPAA Breach Notification Rule, 45 CFR 164.400-414, available at *https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html*.
[8] *Id.*

III. Questions Regarding the HBN Rule

The Commission invites members of the public to comment on any issues or concerns they believe are relevant or appropriate to the Commission's review of the HBN Rule, and to submit written data, views, facts, and arguments addressing the Rule. All comments should be filed as prescribed in the **ADDRESSES** section of this document, and must be received by [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. If your comment proposes any modifications to the Rule, please also address whether your proposed modification may conflict with the statutory provisions of the Recovery Act and, if so, whether you propose seeking legislative changes to the Recovery Act. The Commission is particularly interested in comments addressing the following questions:

A. General Issues

1. Is there a continuing need for specific provisions of the Rule? Why or why not?
2. What benefits has the Rule provided to consumers? What evidence supports the asserted benefits?
3. What modifications, if any, should be made to the Rule to increase the benefits to consumers?
    a. What evidence supports the proposed modifications?
    b. How would these modifications affect the costs the Rule imposes on businesses, including small businesses?
4. What significant costs, if any, has the Rule imposed on consumers? What evidence supports the asserted costs?

5. What modifications, if any, should be made to the Rule to reduce any costs imposed on consumers?
    a. What evidence supports the proposed modifications?
    b. How would these modifications affect the benefits provided by the Rule?
6. What benefits, if any, has the Rule provided to businesses, including small businesses? What evidence supports the asserted benefits?
7. What modifications, if any, should be made to the Rule to increase its benefits to businesses, including small businesses?
    a. What evidence supports the proposed modifications?
    b. How would these modifications affect the costs the Rule imposes on businesses, including small businesses?
    c. How would these modifications affect the benefits to consumers?
8. What significant costs, if any, including costs of compliance, has the Rule imposed on businesses, including small businesses? What evidence supports the asserted costs?
9. What modifications, if any, should be made to the Rule to reduce the costs imposed on businesses, including small businesses?
    a. What evidence supports the proposed modifications?
    b. How would these modifications affect the benefits the Rule provides to consumers?
10. What evidence is available concerning the degree of industry compliance with the Rule?

11. What modifications, if any, should be made to the Rule to account for changes in relevant technology, economic conditions, or laws? For example, as the healthcare industry adopts standardized application programming interfaces ("APIs") to help individuals to access their electronic health information with smartphones and other mobile devices (as required by rules implementing the 21st Century Cures Act[9]), will the number of entities subject to the Commission's HBN Rule increase?
    a. What evidence supports the proposed modifications?
12. Are there modifications or changes the Commission should make to the Rule to address any developments in health care products or services related to COVID-19?
13. Does the Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?
    a. What evidence supports the asserted conflicts?
    b. With reference to the asserted conflicts, should the Rule be modified? If so, why, and how? If not, why not?

B. Specific Issues

1. What evidence exists that the Rule has resulted in under-notification, over-notification, or an efficient level of notification?
2. Section 318.1 provides that the Rule does not apply to HIPAA-covered entities or to any other entity to the extent that it engages in activities as a

[9] 45 CFR parts 170 and 171.

business associate of a HIPAA-covered entity. Has this limitation helped to harmonize the Commission's HBN Rule with HHS's rule? Why or why not?

3. Do the definitions set forth in § 318.2 of the Rule accomplish the Recovery Act's goal of advancing the use of health information technology while strengthening the privacy and security protections for health information?
4. Are the definitions in § 318.2 clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?
5. Should the definition of "PHR identifiable health information" in § 318.2(d) be modified in light of technological advances in methods of de-identification and re-identification? If so, how, consistent with the Act's requirements?
6. Should the definitions of "PHR related entity" in § 318.2(f), "Third party service provider" in § 318.2(h), or "Vendor of personal health records" in Section 318.2(j) be modified in light of changing technological and economic conditions, such as the proliferation of mobile health applications ("apps"), virtual assistants offering health services, and platforms' health tools? If so, how, consistent with the Act's requirements?
7. Section 318.4 sets out the timing requirements for notification. Are these requirements clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?
8. Section 318.5 sets out the requirements for the method of notice of a breach. Are these requirements clear and appropriate? Do technological changes, such as the increased use of in-app messaging, text messages, and platform

messaging, warrant any changes to this section, consistent with the Act's requirements?

9. Section 318.6 sets out the requirements for the content of notice of a breach. Are these requirements clear and appropriate? If not, how can they be improved, consistent with the Act's requirements?
10. What are the implications (if any) for enforcement of the Rule raised by direct-to-consumer technologies and services such as mobile health apps, virtual assistants, and platforms' health tools?

IV. Instructions for Submitting Comments

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Please write "Health Breach Notification Rule, 16 CFR part 318, Project No. P205405" on the comment. Because of the public health emergency in response to the COVID-19 outbreak and the agency's heightened security screening, postal mail addressed to the Commission will be subject to delay. We strongly encourage you to submit your comment online through the *https://www.regulations.gov* website. To ensure the Commission considers your online comment, please follow the instructions on the web-based form provided by *regulations.gov*. Your comment, including your name and your state, will be placed on the public record of this proceeding, including the *https://www.regulations.gov* website.

If you file your comment on paper, please write "Health Breach Notification Rule, 16 CFR part 318, Project No. P205405" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the

Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex B), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street SW, 5th Floor, Suite 5610 (Annex B), Washington, DC 20024.

Because your comment will be placed on the public record, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any "trade secret or any commercial or financial information which . . . . is privileged or confidential" – as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled "Confidential," and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request, and must identify the specific portions of the comment to be withheld from the public record.

Your comment will be kept confidential only if the General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at www.regulations.gov, we cannot redact or remove your comment unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the General Counsel grants that request.

Visit the Commission Website at https://www.ftc.gov to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 90 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. For information on the Commission's privacy policy, including routine uses permitted by the Privacy Act, see https://www.ftc.gov/site-information/privacy-policy.

By direction of the Commission.

April J. Tabor,

Acting Secretary.

[FR Doc. 2020-10263 Filed: 5/21/2020 8:45 am; Publication Date: 5/22/2020]