Supporting Statement for Proposed Amendments to the
Health Breach Notification Rule
16 C.F.R. Part 318
(OMB Control No. 3084-0150)

Overview of Information Collection

The Federal Trade Commission ("FTC" or "Commission") is finalizing amendments to the Health Breach Notification Rule ("Rule"), 16 C.F.R. Part 318. The Rule currently requires vendors of personal health records ("PHR") and PHR related entities that are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") to comply with certain notice requirements in the event of a breach of unsecured personally identifiable health information. The amendments pertain to (1) the scope of the Rule, (2) the methods of notice, and (3) the content of notice, among other issues.

As part of this rulemaking, the Commission issued a Notice of Proposed Rulemaking ("NPRM") in June 2023.[1] Upon publication of the NPRM, the Commission submitted an associated clearance request with Supporting Statement to OMB. In response, OMB filed a Notice of Action requesting that the Commission resubmit the clearance request upon the finalization of the amendments.

(1) & (2) Necessity for and Use of the Information Collection

Section 13407 of the American Recovery and Reinvestment Act of 2009 ("the Recovery Act") directed the Commission to issue a rule requiring vendors of PHRs and related entities that are not covered by HIPAA to notify consumers, the Commission, and, in some cases, the media, of a breach of unsecured PHR identifiable health information. After receiving comments from the public, the FTC issued the Rule in 2009.[2] The Rule imposed notification requirements on three types of entities: (1) PHR vendors; (2) PHR related entities; and (3) third party service providers.

The amendments that the FTC is now finalizing mainly pertain to: (1) the coverage of the rule—specifically, the rule's coverage of developers of many health applications ("apps") and similar technologies; (2) methods of notice; and (3) the content of notice. These amendments are needed to ensure that entities covered by the Rule understand their obligations under the Rule, giving important guidance to the marketplace on the Rule's scope.

(3) Information Technology

The final rule gives explicit examples of electronic options that covered entities may use to provide notice to consumers. For example, the final rule will permit covered entities in certain circumstances to notify consumers via email in combination with one or more of the following: text message; within-application messaging; or electronic banner. These electronic options will

[1] 88 FR 37819 (June 9, 2023).
[2] 74 FR 42962 (Aug. 25, 2009).

help minimize the burden and cost of the final rule's information collection requirements for entities subject to the Rule. They are consistent with the Government Paperwork Elimination Act ("GPEA"), 44 U.S.C. § 3504, which, in relevant part, requires that OMB ensure that Executive agencies provide for the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper.

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would duplicate the amendments. The Department of Health and Human Services' ("HHS") Breach Notification Rule, 45 C.F.R. §§ 164.400-414, addresses breaches of unsecured protected health information in the context of entities covered by HIPAA. However, the FTC's Rule does not apply to HIPAA-covered entities, or to any other entity to the extent it engages in activities as a business associate of a HIPAA-covered entity, and the amendments do not change this fact.

(5) Efforts to Minimize Small Organization Burden

In drafting the amendments, the Commission made every effort to avoid unduly burdensome requirements for small entities. In particular, the Commission believes that (1) the alternative of providing notice to consumers electronically, and (2) adjusting the notification timeline for entities to report to the FTC breaches of security involving 500 or more individuals (i.e., from without unreasonable delay and in no case later than 10 calendar days after the discovery of a breach of security to without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security) will assist small entities by significantly reducing the cost of sending breach notices and the burden associated with investigating and reporting breaches in a timely manner.

(6) Consequences of Conducting Collection Less Frequently

The Recovery Act directed the Commission to establish a regime for the reporting of breaches of unsecured personally identifiable health data. A less frequent "collection" would violate both the intent and purpose of the Recovery Act because breaches that should otherwise be reported would not be reported or not be reported timely.

(7) Circumstances Requiring Collection Inconsistent with PRA Guidelines

The collection of information is consistent with all applicable guidelines contained in 5 C.F.R. § 1320.5(d)(2).

(8) Public Comments/Consultation Outside the Agency

Dating back to the Rule's inception, the Commission has a long history of consultation with external stakeholders, including affected entities and consumers. In May 2020, the Commission announced its regular, ten-year review of the Rule and requested public comment about potential Rule changes.[3] The Commission sought public comment on, among other things,

[3] 85 FR 31085 (May 22, 2020).

whether changes should be made to the Rule in light of technological changes, such as the proliferation of apps and similar technologies. The Commission received 26 public comments.[4]

On June 9, 2023, the Commission issued an NPRM proposing to revise the Rule in seven ways.[5] The Commission received approximately 120 comments in response to the NPRM from a wide spectrum of stakeholders, including consumers, consumer groups, trade associations, think tanks, policy organizations, private sector entities, and members of Congress.[6]

The Commission is now finalizing the amendments. The Commission believes that the amendments are consistent with the language and intent of the Recovery Act, address the concerns raised by the public comments in response to the NPRM,[7] and will ensure that the Rule remains current in the face of changing business practices and technological developments. The burden analyses in the final rule and below have been updated to reflect recent increases in wage rates, the number of covered entities, and the number of breaches per year.

(9) Payments or Gifts to Respondents

Not applicable.

(10) & (11) Assurances of Confidentiality/Matters of a Sensitive Nature

Neither the amendments' breach notification requirements nor the associated form involves disclosures of confidential or sensitive information.

(12) Estimated Annual Hours Burden and Associated Labor Costs

The PRA burden of the amendments depends on a variety of factors, including the

[4] Comments are available at *https://www.regulations.gov/docket/FTC-2020-0045/comments*.

[5] 88 FR 37819.

[6] Comments are available at *https://www.regulations.gov/document/FTC-2023-0037-0001/comment*.

[7] Although the Commission did not propose any timing changes in the NPRM, the Commission requested comments on several issues related to timing, including the timing of the notification to the FTC. Several commenters expressed support for extending the notification timeline to the FTC. Commenters provided several reasons why the existing requirement of notice to the FTC "as soon as possible and in no case later than ten business days following the date of discovery of the breach" for breaches involving 500 or more individuals should be amended. For example, commenters noted that ten days does not provide entities with sufficient time to adequately investigate incidents and fully understand the facts, possibly leading to notices that may be incomplete and require amendment or correction. Others commented that the existing requirement diverts key resources from investigating potential breaches, indicating that when a breach is suspected or has been discovered, the target entity's focus should be responding to the incident, conducting a thorough investigation of what may have occurred, and addressing and mitigating vulnerabilities to ensure additional information is not compromised. Having considered the public comments, the Commission agrees with commenters who recommended that the notification timeline to the FTC for breaches of security involving 500 or more individuals should be adjusted. The Commission agrees that in certain incidents, especially large, complex breaches, it can be challenging for entities to fully understand the scope of a breach in ten business days, leading to the possibility of incomplete breach notices. Accordingly, the amendments require entities, for breaches involving 500 or more individuals, to notify the FTC contemporaneously with the notice sent to affected individuals pursuant to § 318.4(a) – i.e., without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

number of covered firms; the percentage of such firms that will experience a breach requiring further investigation and, if necessary, the sending of breach notices; and the number of consumers notified. The annual hours and cost estimates below likely overstate the burden because, among other things, they assume that all covered firms experiencing breaches subject to the amendments' notification requirements will be required to take all of the steps described below. However, not all breaches will require covered firms to take all the steps described below.

The analysis may also overstate the burden of the amendments' requirements because it assumes that covered firms would not take any of the steps described were it not for the requirements of the amendments. For example, the analysis incorporates labor costs associated with understanding what information has been breached. It seems likely that some firms would incur such costs even in the absence of the amended Rule's requirements because the firms are independently interested in identifying, understanding, and remediating security risks. A company that investigates, for its own purposes, what information has been breached is unlikely to fully duplicate the costs of that investigation in complying with the amended Rule. Therefore, it may not be correct in all cases that complying with the amended Rule results in added labor costs for this activity. Nevertheless, in order to allow for a complete understanding of all the potential costs associated with compliance, these costs are included in this analysis.

Based on industry reports, FTC staff estimates that the amendments' information collection requirements will cover approximately 193,000 entities, which, in the event of a breach, may be required to notify consumers, the Commission, and in some cases, the media. As of March 2024, there are approximately 1.8 million apps in the Apple App Store[8] and 2.4 million apps in the Google Play Store.[9] It appears that roughly 193,000 of the apps offered in either store are categorized as "Health and Fitness."[10] This figure serves as a rough proxy for all covered PHRs, because most websites and connected health devices that will be subject to the amended Rule act in conjunction with an app.

FTC staff estimates that these 193,000 entities will, cumulatively, experience 82 breaches per year for which notification may be required. With the proviso that there is insufficient data at this time about the number and incidence rate of breaches at entities covered by the amended Rule (due to underreporting prior to issuance of the Commission's September 15, 2021 Policy Statement[11] clarifying that many health apps and connected devices not covered by HIPAA are covered by the FTC's 2009 Rule), FTC staff determined the number of estimated breaches by

---

[8] *See* App Store – Apple, https://www.apple.com/app-store/.

[9] *See* AppBrain: Number of Android Apps on Google Play (Mar 2024) *https://www.appbrain.com/stats/number-of-android-apps*.

[10] *See* Business of Apps, "App Data Report: App Store Stats, Downloads, Revenues and App Rankings," *https://www.businessofapps.com/data/report-app-data/* (reporting 90,913 apps in the Apple iOS App Store and 102,402 apps in the Google Play Store that were categorized as "Health and Fitness"). Together, this suggests there are approximately 193,000 Health and Fitness apps. This figure is likely both under- and over-inclusive as a proxy for covered entities. For example, this figure does not include apps categorized elsewhere (i.e., outside "Health and Fitness") that may be PHRs. However, at the same time, this figure also overestimates the number of covered entities, since many developers make more than one app and may specialize in the Health and Fitness category.

[11] Statement of the Commission on Breaches by Health Apps and Other Connected Devices, Fed. Trade Comm'n (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf ("Policy Statement").

calculating the breach incidence rate for HIPAA-covered entities, and then applied this rate to the estimated total number of entities that will be subject to the amended Rule.[12] Additionally, as the number of breaches per year grew significantly in the recent years,[13] and FTC staff expects this trend to continue, FTC staff relied on the average number of breaches in 2021 through 2023 to estimate the annual breach incidence rate for HIPAA-covered entities.

Specifically, the HHS Office for Civil Rights ("OCR") reported 715 breaches in 2021 719 breaches in 2022, and 733 breaches in 2023,[14] which results in an average of 722 breaches between 2021 and 2023. Based on the 1.7 million entities that are covered by the HIPAA Breach Notification Rule[15] and the average number of breaches for 2021 through 2023, FTC staff determined an annual breach incidence rate of 0.000425 (722 / 1.7 million). Accordingly, multiplying the breach incidence rate (0.000425) by the estimated number of entities covered by the amendments' information collection requirements (193,000) results in an estimated 82 breaches per year.

Estimated Annual Burden Hours: 12,300

Estimated Annual Labor Costs: $883,140

First, to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission,[16] FTC staff estimates that covered firms will require per breach, on average, 150 hours of employee labor at a cost of $10,770.[17] This estimate does not include the cost of equipment or other tangible assets of the

[12] FTC staff used information publicly available from HHS on HIPAA related breaches because the HIPAA Breach Notification Rule is similarly constructed. However, while there are similarities between HIPAA-covered entities and HBNR-covered entities, it is not necessarily the case that rates of breaches would follow the same pattern. For instance, HIPAA-covered entities are generally subject to more stringent data security requirements under HIPAA, but also may be more likely targets for security incidents (*e.g.*, ransomware attacks on hospitals and other medical treatment centers covered by HIPAA have increased dramatically in recent years); thus, this number could be an under- or overestimate of the number of potential breaches per year.

[13] According to the HHS Office for Civil Rights ("OCR"), the number of breaches per year grew from 358 in 2017 to 733 breaches in 2023. *See Breach Portal*, U.S. Dep't of Health & Human Servs., Office for Civil Rights, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf* (last visited March 1, 2024). The data was downloaded on March 1, 2024, resulting in limited data for 2024. Thus, breaches from 2024 were excluded from the calculations. However, breach investigations that remain open (under investigation) from years prior to 2024 are included in the count of yearly breaches.

[14] *See Breach Portal*, U.S. Dep't of Health & Human Servs., Office for Civil Rights, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf* (last visited March 1, 2024).

[15] In a Federal Register Notice ("FRN") on Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, OCR proposes increasing the number of covered entities from 700,000 to 774,331. 86 FR 6446, 6497 (Jan. 21, 2021). For purposes of calculating the annual breach incidence rate, FTC staff utilized 700,000 covered entities because the proposed estimate of 774,331 covered entities represents a projected increase that has not been finalized by OCR. The FRN also lists the number of covered Business Associates as 1,000,000. *Id.* at 6528. FTC staff arrived at 1.7 million entities subject to the HIPAA Breach Notification Rule by adding 700,000 covered entities and 1,000,000 Business Associates.

[16] An updated version of the reporting form is enclosed with the information collection requests ("ICRs").

[17] This estimate is the sum of 40 hours of marketing managerial time (at an average wage of $76.10), 40 hours of computer programmer time ($49.42), 20 hours of legal staff ($78.74), and 50 hours of computer and information

breached firms because they will likely use the equipment and other assets they have for ordinary business purposes. Based on the estimate that there will be 82 breaches per year, the annual hours of burden for affected entities will be 12,300 hours (150 hours x 82 breaches) with an associated labor cost of $883,140 (82 breaches × $10,770).

(13) Estimated Capital/Other Non-Labor Costs Burden

The capital and non-labor costs associated with breach notifications depends upon the number of consumers contacted and whether covered firms are likely to retain the services of a forensic expert. For breaches affecting large numbers of consumers, covered firms are likely to retain the services of a forensic expert.

FTC staff estimates that, for each breach requiring the services of forensic experts, forensic experts may spend approximately 40 hours to assist in the response to the cybersecurity intrusion, at an estimated cost of $20,000.[18] FTC staff estimates that the services of forensic experts will be required in 60% of the 82 breaches. Based on the estimate that there will be 49 breaches per year requiring forensic experts (60% × 82 breaches), the annual hours burden for affected entities will be 1,960 hours (49 breaches requiring forensic experts × 40 hours) with an associated cost of $980,000 (49 breaches requiring forensic experts × $20,000).

Using the data on HIPAA-covered breach notices available from HHS for the years 2018-2023, FTC staff estimates that the average number of individuals affected per breach is 93,497. Given an estimated 82 breaches per year, FTC staff estimates an average of 7,666,754 consumers per year will receive a breach notification (82 breaches × 93,497 individuals per breach).

Based on a recent study of data breach costs, FTC staff estimates the cost of providing notice to consumers to be $11.87 per breached record.[19] This estimate includes the costs of electronic notice, letters, outbound calls or general notice to data subjects; and engagement of outside experts. Applied to the above-stated estimate of 7,666,754 consumers per year receiving breach notification yields an estimated total annual cost for all forms of notice to consumers of $91,004,370 (7,666,754 consumers × $11.87 per record). Accordingly, the estimated capital and non-labor costs total $91,984,370 ($980,000 + $91,004,370).

---

systems managerial time ($83.49). *See* Occupational Employment and Wage Statistics, U.S. Bureau of Labor Statistics (May 2022), *https://www.bls.gov/oes/current/oes_nat.htm#00-0000*.

[18] This estimate is the sum of 40 hours of forensic expert time at a cost of $500 per hour, which yields a total cost of $20,000 (40 hours × $500/hour).

[19] *See* IBM Security, Costs of a Data Breach Report 2023 (2023), *https://www.ibm.com/reports/data-breach* ("2023 IBM Security Report"). The research for the 2023 IBM Security Report is conducted independently by the Ponemon Institute, and the results are reported and published by IBM Security. Figure 2 of the 2023 IBM Security Report shows that cost per record of a breach was $165 per record in 2023, $164 in 2022, and $161 in 2021, resulting in an average cost of $163.33. Figure 5 of the 2023 IBM Security Report shows that 8.3% ($0.37m/$4.45m) of the average cost of a data breach are due to "Notification" costs. The fraction of average breach costs due to "Notification" were 7.1% in 2022 and 6.4% in 2021 (IBM Security, Costs of a Data Breach Reports 2022 and 2021). Using the average of these numbers (7.27%), FTC staff estimates that notification costs per record across the three years are 7.27% × $163.33 = $11.87 per record.

(14) Estimate of Cost to Federal Government

FTC staff estimates that the cost to the FTC Bureau of Consumer Protection of enforcing the Rule's notification requirements will be approximately $150,000 per year. This estimate is based on the assumption that 50% of the work year of two FTC attorneys will be expended to enforce the Rule's requirements related to notification. Employee benefits, as well as clerical and other support services, are also included in this estimate.

(15) Changes in Burden

The amendments will result in an estimated 12,300 hours of burden, $883,140 in associated annual labor costs, and $91,984,370 in annual capital and/or other non-labor related costs.

(16) Plans for Tabulation and Publication

There are no plans to publish for statistical use any information collected under the amended Rule. However, the Commission intends to compile the information it receives about breaches affecting 500 or more individuals, which the Commission will update periodically and make publicly available.[20]

(17) Failure to Display of Expiration Date for OMB Approval

Not applicable. The expiration date will be displayed on relevant forms.

(18) Exceptions to the Certification for Paperwork Reduction Act Submissions

The FTC certifies that this collection of information is consistent with the requirements of 5 C.F.R. § 1320.9, and the related provisions of 5 C.F.R. § 1320.8(b)(3), and is not seeking an exemption to these certification requirements.

[20] The Commission publishes a list of breaches involving 500 or more individuals, and the Commission periodically updates this list. *See* FTC, *Notices Received by the FTC Pursuant to the Health Breach Notification Rule* (last visited Mar. 26, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Health%20Breach%20Notices%20Received%20by%20the%20FTC.pdf.