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

Overview of Information Collection

The Federal Trade Commission ("FTC" or "Commission") proposes 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. Among others, the proposed amendments pertain to (1) the scope of the Rule, (2) the methods of notice, and (3) the content of notice. The proposed amendments would result in the following information collection burdens.

(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 personal health records ("PHRs") and related entities that by the Health Information Portability and Accountability Act ("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,[1] which imposed notification requirements on three types of entities: PHR vendors; PHR related entities; and third party service providers.

The proposed amendments pertain to, among others: (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 proposed 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 Rule gives explicit examples of electronic options that covered entities may use to provide notice to consumers. For example, the proposed amendments would 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 help minimize the burden and cost of the 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.

[1] 74 FR 42962 (Aug. 25, 2009).

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would duplicate the proposed Rule. 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 proposed amendments do 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.

(5) Efforts to Minimize Small Organization Burden

In drafting the proposed amendments, the Commission made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the alternative of providing notice to consumers electronically will assist small entities by significantly reducing the cost of sending breach notices.

(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 in the Rule is consistent with all applicable guidelines contained in 5 C.F.R. § 1320.5(d)(2).

(8) Public Comments/Consultation Outside the Agency

The Commission is seeking public comment on the proposed requirements and the associated PRA analysis. Section IV of the NPRM addresses the proposed information collection requirement.

(9) Payments or Gifts to Respondents

Not applicable.

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

Neither the Rule's 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 proposed requirements depends on a variety of factors, including

the 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, though it is not necessarily so, that all covered firms experiencing breaches subject to the Rule's notification requirements will be required to take all of the steps described below.

The analysis may also overstate the burden of the proposed Rule's requirements because it assumes that covered firms would not take any of the steps described were it not for the requirements of the proposed Rule. 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 proposed 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 proposed Rule. Therefore, it may not be correct in all cases that complying with the proposed 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, staff estimates that the Commission's proposed information collection requirements will cover approximately 170,000 entities, which, in the event of a breach, may be required to notify consumers and the Commission. As of November 2022, there are approximately 1.8 million apps in the Apple App Store[2] and 2.7 million apps in the Google Play Store.[3] It appears that roughly 170,000 of the apps offered in either store are categorized as "Health and Fitness."[4] This figure serves as a rough proxy for all covered PHRs, because most websites and connected health devices that would be subject to the Rule act in conjunction with an app.

Staff estimates that these 170,000 entities will, cumulatively, experience 71 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 Commission's Rule (due to underreporting prior to issuance of the Commission's September 15, 2021 Policy Statement[5] clarifying that many health apps and similar technologies not covered by HIPAA are covered by the FTC's existing Rule), staff determined the number of estimated breaches by calculating the breach incidence rate for HIPAA-covered entities, and then applied

---

[2] *See* App Store – Apple, https://www.apple.com/app-store/ and App Store Data (2023) – Business of Apps, https://www.businessofapps.com/data/app-stores/.

[3] App Store Data (2023) – Business of Apps, https://www.businessofapps.com/data/app-stores/.

[4] *See* App Store Data (2023), *supra* note 2, which reports 78,764 apps in the Apple App Store and 91,743 apps in the Google Play Store were categorized as "Health and Fitness" apps as of November 2022. This figure is likely both under- and over-inclusive. 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.

[5] 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").

this rate to the estimated total number of entities that will be subject to the proposed Rule.[6] Additionally, as the number of breaches per year grew significantly in the recent years,[7] and staff expects this trend to continue, staff relied on the average number of breaches in 2021 and 2022 to estimate the annual breach incidence rate for HIPAA-covered entities.

Specifically, the HHS Office for Civil Rights ("OCR") reported 715 breaches in 2021 and 717 breaches in 2022,[8] which results in an average of 716 of breaches for 2021 and 2022. Based on the 1.7 million entities that are covered by the HIPAA Breach Notification Rule[9] and the average number of breaches for 2021 and 2022, staff determined an annual breach incidence rate of 0.00042 (716 / 1.7 million). Accordingly, multiplying the breach incidence rate (0.00042) by the estimated number of entities covered by the proposed information collection requirements (170,000) results in an estimated 71 breaches per year.

Estimated Annual Burden Hours: 10,650

Estimated Annual Labor Costs: $720,579

First, to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission, staff estimates that covered firms will require per breach, on average, 150 hours of employee labor at a cost of $10,149.[10] This estimate does not include the cost of equipment or other tangible assets of the breached firms because they likely will use the equipment and other assets they have for ordinary business purposes. Based on the estimate that there will be 71 breaches per year the annual hours of burden for affected entities will be 10,650 hours (150 hours x 71 breaches) with an associated labor cost of $720,579 (71 breaches × $10,149).

---

[6] 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 stronger 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.

[7] According to the HHS Office for Civil Rights ("OCR"), the number of breaches per year grew from 358 in 2017 to 715 breaches in 2021 and 717 breaches in 2022. *See Breach Portal*, U.S. Dep't of Health & Human Servs., Office for Civil Rights, https://ocrportal hhs.gov/ocr/breach/breach_report.jsf (visited on March 2, 2023). The data was downloaded on March 2, 2023, resulting in limited data for 2023. Thus, breaches from 2023 were not considered. However, breach investigations that remain open (under investigation) are included in the count of yearly breaches.

[8] *See Breach Portal*, U.S. Dep't of Health & Human Servs., Office for Civil Rights, https://ocrportal hhs.gov/ocr/breach/breach_report.jsf (visited on March 2, 2023).

[9] In a recent 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). The FRN also lists the number of covered Business Associates as 1,000,000 (Table 2).

[10] This estimate is the sum of 40 hours of marketing managerial time (at an average wage of $73.77), 40 hours of computer programmer time ($46.46), 20 hours of legal staff ($71.17), 50 hours of computer and information systems managerial time ($78.33). *See* Occupational Employment and Wage Statistics, U.S. Bureau of Labor Statistics (May 2021), https://www.bls.gov/oes/current/oes_nat.htm#00-0000.

(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.[11] FTC staff estimates that the services of forensic experts will be required in 60% of the 71 breaches. Based on the estimate that there will be 43 breaches per year requiring forensic experts (60% × 71 breaches), the annual hours burden for affected entities will be 1,720 hours (43 breaches requiring forensic experts × 40 hours) with an associated cost of $860,000 (43 breaches requiring forensic experts × $20,000).

Using the data on HIPAA-covered breach notices available from HHS for the years 2021-2022, FTC staff estimates that the average number of individuals affected per breach is 62,402.[12] Given an estimated 71 breaches per year, FTC staff estimates an average of 4,430,542 consumers per year will receive a breach notification (71 breaches × 62,402 individuals per breach).

Based on a recent study of data breach costs, staff estimates the cost of providing notice to consumers to be $10.97 per breached record.[13] This estimate includes the costs of electronic notice, letters, outbound calls or general notice to data subjects; and engagement of outside experts.[14] Applied to the above-stated estimate of 4,430,542 consumers per year receiving breach notification yields an estimated total annual cost for all forms of notice to consumers of $48,603,046 (4,430,542 consumers × $10.97 per record). The estimated capital and non-labor costs total $49,463,046 ($860,000 + $48,603,046).

(14) Estimate of Cost to Federal Government

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 two FTC attorney's work year will be expended to enforce

---

[11] 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).

[12] HHS Breach Data, *supra* note 8 (mean of Individuals Affected during breaches 2017-2022). This analysis uses the last six years of HHS breach data to generate the average, in order to account for the variation in number of individuals affected by breaches observed in the HHS data over time.

[13] *See* IBM Security, Costs of a Data Breach Report 2022 (2022), https://www.ibm.com/reports/data-breach ("2022 IBM Security Report"). The research for the 2022 IBM Security Report is conducted independently by the Ponemon Institute, and the results are reported and published by IBM Security. Figure 2 of the 2022 IBM Security Report shows that cost per record of a breach was $164 per record in 2022 and $161 in 2021, resulting in an average cost of $162.50. Figure 5 of the 2022 IBM Security Report shows that 7.1% ($0.31m / $4.35m) of the average cost of a data breach are due to "Notification" costs. The fraction of average breach costs due to "Notification" were 6.4% the previous year (IBM Security, Costs of a Data Breach Report 2021). Using the average of these numbers, staff estimates that notification costs per record across the two years are 6.75% × $162.50 = $10.97 per record.

[14] *See* 2022 IBM Security Report, *id.* at 54.

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 proposed amendments to the Rule will result in an estimated 10,650 hours of burden, $720,579 in associated annual labor costs, and $49,463,046 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 required by the Rule, but the Commission intends to input the information it receives about breaches affecting 500 or more individuals into a database, which it will update periodically and make publicly available.

(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 CFR 1320.9, and the related provisions of 5 CFR 1320.8(b)(3), and is not seeking an exemption to these certification requirements.