Billing Code: 6750-01P

FEDERAL TRADE COMMISSION

16 CFR Part 318

RIN 3084-AB56

Health Breach Notification Rule

AGENCY: Federal Trade Commission.

ACTION: Final rule.

SUMMARY: The Federal Trade Commission ("FTC" or "Commission") is amending the Commission's Health Breach Notification Rule (the "HBN Rule" or the "Rule"). The HBN Rule 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. The amendments: (1) clarify the Rule's scope, including its coverage of developers of many health applications ("apps"); (2) clarify what it means for a vendor of personal health records to draw PHR identifiable health information from multiple sources; (3) revise the definition of breach of security to clarify that a breach of security includes data security breaches and unauthorized disclosures; (4) revise the definition of PHR related entity; (5) modernize the method of notice; (6) expand the content of the notice; (7) alter the Rule's timing requirement for notifying the FTC of a breach of security; and (8) improve the Rule's readability by clarifying cross-references and adding statutory citations, consolidating notice and timing requirements, articulating the penalties for non-compliance, and incorporating a small number of non-substantive changes.

DATES: The amendments are effective [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Relevant portions of the record of this proceeding, including this document, are available at https://www.ftc.gov and https://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: Ryan Mehm, (202) 326-2918, rmehm@ftc.gov, and Ronnie Solomon, (202) 326-2098, rsolomon@ftc.gov, Bureau of Consumer Protection, Federal Trade Commission.

SUPPLEMENTARY INFORMATION:

I. Background

Congress enacted the American Recovery and Reinvestment Act of 2009 ("Recovery Act" or "the Act"),[1] in part to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information. Recognizing that certain entities that hold or interact with consumers' personal health records were not subject to the privacy and security requirements of HIPAA,[2] Congress created requirements for such entities to notify individuals, the Commission, and, in some cases, the media of the breach of unsecured identifiable health information from those records.

Specifically, section 13407 of the Recovery Act created certain protections for "personal health records" or "PHRs,"[3] electronic records of PHR identifiable health information on an individual that can be drawn from multiple sources and that are managed, shared, and controlled by or primarily for the individual.[4] Congress 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 personal health records) were collecting

[1] Am. Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009).
[2] Health Ins. Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936 (1996).
[3] 42 U.S.C. 17937.
[4] 42 U.S.C. 17921(11).

consumers' health information but were not subject to the privacy and security requirements of HIPAA. Accordingly, the Recovery Act directed the FTC to issue a rule requiring these non-HIPAA covered entities, and their third party service providers, to provide notification of any breach of unsecured PHR identifiable health information. The Commission issued its Rule implementing these provisions in 2009.[5] FTC enforcement of the Rule began on February 22, 2010.

The Rule that the Commission issued in 2009 ("2009 Rule") requires vendors of personal health records and PHR related entities to provide: (1) notice to consumers whose unsecured PHR identifiable health information has been breached; (2) notice to the Commission; and (3) notice to prominent media outlets[6] serving a State or jurisdiction, in cases where 500 or more residents are confirmed or reasonably believed to have been affected by a breach.[7] The Rule also requires third party service providers (i.e., those companies that provide services such as billing, data storage, attribution, or analytics) to vendors of personal health records and PHR related entities to provide notification to such vendors and entities following the discovery of a breach.[8]

The 2009 Rule requires notice to individuals "without unreasonable delay and in no case later than 60 calendar days" after discovery of a data breach.[9] 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.[10] The FTC makes available a standard form for

[5] 74 FR 42962 (Aug. 25, 2009) ("2009 Final Rule").
[6] The Recovery Act does not limit this notice to particular types of media. Thus, an entity can satisfy the requirement to notify ''prominent media outlets'' by, for example, disseminating press releases to a number of media outlets, including internet media in appropriate circumstances, where most of the residents of the relevant state or jurisdiction get their news. This will be a fact-specific inquiry that will depend on what media outlets are "prominent" in the relevant jurisdiction. 74 FR 42974.
[7] 16 CFR 318.3, 318.5.
[8] *Id.* 318.3(b).
[9] *Id.* 318.4(a).
[10] *Id.* 318.5(c).

companies to use to notify the Commission of a breach,[11] and posts a list of breaches involving 500 or more individuals on its website.[12]

The 2009 Rule applies only to breaches of "unsecured" health information, which the Rule defines as health information that is not secured through technologies or methodologies specified by the Department of Health and Human Services ("HHS"). The Rule does not apply to businesses or organizations covered by HIPAA.[13] HIPAA-covered entities and their "business associates" must instead comply with HHS's breach notification rule.[14]

Since the Rule's issuance, apps and other direct-to-consumer health technologies, such as fitness trackers and wearable blood pressure monitors, have become commonplace.[15] Further, as an outgrowth of the COVID-19 pandemic, consumer use of such health-related technologies has increased significantly.[16]

---

[11] Fed. Trade Comm'n, Notice of Breach of Health Information, *https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/health_breach_form.pdf*.

[12] Fed. Trade Comm'n, Notices Received by the FTC Pursuant to the Health Breach Notification Rule, *https://www.ftc.gov/system/files/ftc_gov/pdf/Health%20Breach%20Notices%20Received%20by%20the%20FTC.pdf* (last visited Dec. 2, 2022).

[13] Per HHS guidance, electronic health information is "secured" if it has been encrypted according to certain specifications set forth by HHS, or if the media on which electronic health information has been stored or recorded is destroyed according to HHS specifications. *See* 74 FR 19006; *see also* U.S. Dep't of Health & Human Servs., *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (July 26, 2013), *https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html*. PHR identifiable health information would be considered "secured" if such information is disclosed by, for example, a vendor of personal health records, to a PHR related entity or a third party service provider, in an encrypted format meeting HHS specifications, and the PHR related entity or third party service provider stores the data in an encrypted format that meets HHS specifications and also stores the encryption and/or decryption tools on a device or at a location separate from the data.

[14] 45 CFR 164.400-414.

[15] *See*, *e.g.*, Kokou Adzo, *App Development in Healthcare: 12 Exciting Facts*, TechnoChops (Jan. 3, 2023), *https://www.technochops.com/programming/4329/app-development-in-healthcare/*; Emily Olsen, *Digital health apps balloon to more than 350,000 available on the market, according to IQVIA report*, MobiHealthNews (Aug. 4, 2021), *https://www.mobihealthnews.com/news/digital-health-apps-balloon-more-350000-available-market-according-iqvia-report;* Elad Natanson, *Healthcare Apps: A Boon, Today and Tomorrow*, Forbes (July 21, 2020), *https://www.forbes.com/sites/eladnatanson/2020/07/21/healthcare-apps-a-boon-today-and-tomorrow/?sh=21df01ac1bb9*.

[16] *See id. See also* Lis Evenstad, *Covid-19 has led to a 25% increase in health app downloads, research shows*, ComputerWeekly.com (Jan. 12, 2021), *https://www.computerweekly.com/news/252494669/Covid-19-has-led-to-a-*

In May 2020, the Commission announced its regular, ten-year review of the Rule and requested public comment about potential Rule changes.[17] The Commission requested comment on, among other things, 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.[18]

Many of the commenters in 2020 encouraged the Commission to clarify that the Rule applies to apps and similar technologies.[19] In fact, no commenter opposed this type of clarification regarding the Rule's coverage of health apps. Several commenters pointed out examples of health apps that have abused users' privacy, such as by disclosing sensitive health information without consent.[20] Several commenters noted the urgency of this issue, as consumers have further embraced digital health technologies during the COVID-19 pandemic.[21] Commenters argued that the Commission should take additional steps to protect unsecured PHR identifiable health information that is not covered by HIPAA, both to prevent harm to consumers[22] and to level the competitive playing field among companies dealing with the same

25-increase-in-health-app-downloads-research-shows (finding that COVID-19 has led to a 25% increase in health app downloads); Jasmine Pennic, *U.S. Telemedicine App Downloads Spikes During COVID-19 Pandemic,* HIT Consultant (Sept. 8, 2020), *https://hitconsultant.net/2020/09/08/u-s-telemedicine-app-downloads-spikes-during-covid-19-pandemic/* ("US telemedicine app downloads see dramatic increases during the COVID-19 pandemic, with some seeing an 8,270% rise YoY.").

[17] 85 FR 31085 (May 22, 2020).

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

[19] *E.g.*, Am. Health Info. Mgmt. Ass'n ("AHIMA") at 2; Kaiser Permanente at 3; Allscripts at 3; Am. Acad. of Ophthalmology at 2; All. for Nursing Informatics ("ANI") at 2; Am. Med. Ass'n ("AMA") at 4; Am. Coll. of Surgeons at 6; Physicians' Elec. Health Rec. Coal. ("PEHRC") at 4 ("Apps that collect health information, regardless of whether or not they connect to an EHR, must be regulated by the FTC Health Breach Notification Rule to ensure the safety and security of personal health information."); Am.'s Health Ins. Plans ("AHIP") and Blue Cross Blue Shield Ass'n ("BCBS") at 2; The App Ass'n's Connected Health Initiative ("CHI") at 3.

[20] Kaiser Permanente at 7; The Light Collective at 2; Am. Acad. of Ophthalmology at 2; PEHRC at 2-3.

[21] Lisa McKeen at 2-3; Kaiser Permanente at 7-8; AMA at 3; Off. of the Att'y Gen. for the State of Cal. ("OAG-CA") at 3–4; Healthcare Info. and Mgmt. Sys. Soc'y ("HIMSS") and Personal Connected Health All. ("PCH Alliance") at 4–5.

[22] Georgia Morgan; Am. Acad. of Ophthalmology at 2-3 (arguing that consumers do not know all the ways their data is being used by third parties, and the downstream consequences of data being used in this way may ultimately erode

health information.[23] To that end, commenters not only urged the Commission to revise the Rule, but also to increase its enforcement efforts.[24]

1. The Commission's 2021 Policy Statement

On September 15, 2021, the Commission issued a Policy Statement providing guidance on the scope of the Rule. The Policy Statement clarified that the Rule covers most health apps and similar technologies that are not covered by HIPAA.[25] The Rule defines a "personal health record" as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[26] As the Commission explained in the Policy Statement, many makers and purveyors of health apps and other connected devices are vendors of personal health records covered by the Rule because their products are electronic records of PHR identifiable health information.

---

a patient's privacy and willingness to disclose information to his or her physician); Coll. of Healthcare Info. Mgmt. Exec.'s ("CHIME") at 3 (arguing that apps' privacy practices impact the patient-provider relationship because providers do not know what technologies are sufficiently trustworthy for their patients); AMA at 2–3 (expressing concern that patients share less health data with health care providers, perhaps because of "spillover from privacy and security breaches").

[23] Kaiser Permanente at 2, 4; Workgroup for Elec. Data Interchange ("WEDI") at 2; AHIP and BCBS at 3 ("[HIPAA] covered entities, such as health plans, that use or disclose protected health information should not be subject to stricter notification requirements than those imposed on vendors of personal health records or other such entities. Otherwise, the federal government will be providing market advantages to particular industry segments with the effect of dampening competition and harming consumers.").

[24] Kaiser Permanente at 4; Fred Trotter at 1; Casey Quinlan at 1; CARIN Alliance at 2. At the time of this Federal Register notice, the Commission has brought two enforcement actions under the Rule; the first against digital health company GoodRx Holdings, Inc., and the second against an ovulation-tracking mobile app marketed under the name "Premom" and developed by Easy Healthcare, Inc. *United States v. GoodRx Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. Feb. 17, 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc*; *United States v. Easy Healthcare Corp.*, No. 1:23-cv-3107 (N.D. Ill. June 22, 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v*.

[25] 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").

[26] 16 CFR 318.2(d).

The Commission explained that PHR identifiable health information includes individually identifiable health information created or received by a health care provider,[27] and that "health care providers" include any entities that "furnish[] health care services or supplies."[28] Because these health app purveyors furnish health care services to their users through the mobile applications they provide, the information held in the app is PHR identifiable health information, and therefore many health app purveyors likely qualify as vendors of personal health records.[29]

The Policy Statement further explained that the statute directing the FTC to promulgate the Rule requires that a "personal health record" be an electronic record that can be drawn from multiple sources.[30] Accordingly, health apps and similar technologies likely qualify as personal health records covered by the Rule if they are capable of drawing information from multiple sources. The Commission further clarified that health apps and other products experience a "breach of security" under the Rule when they disclose users' sensitive health information without authorization;[31] a breach is "not limited to cybersecurity intrusions or nefarious behavior."[32]

---

[27] *Id.* 318.2(e), incorporating in part the definition from section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)).
[28] *Id.* 318.2(e); 42 U.S.C. 1320d(6), d(3).
[29] *See* Policy Statement at 1.
[30] The Policy Statement provided this example: "[I]f a blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar), it is covered under the Rule." *Id*. at 2.
[31] 16 CFR 318.2(a).
[32] Policy Statement at 2. *See also* Statement of Basis and Purpose to the 2009 Final Rule published in the Federal Register ("2009 Rule Commentary") ("On a related issue, the final rule provides that a breach of security means acquisition of information without the authorization 'of the individual.' Some commenters raised questions about how the extent of individual authorization should be determined. For example, if a privacy policy contains buried disclosures describing extensive dissemination of consumers' data, could consumers be said to have authorized such dissemination?
The Commission believes that an entity's use of information to enhance individuals' experience with their PHR would be within the scope of the individuals' authorization, as long as such use is consistent with the entity's

2. Enforcement History

In 2023, the Commission brought its first enforcement actions under the Rule against vendors of personal health records. In February 2023, the Commission brought an enforcement action alleging a violation of the Rule against GoodRx Holdings, Inc. ("GoodRx"), a digital health company that sells health-related products and services directly to consumers, including prescription medication discount products and telehealth services through its website and mobile applications.[33]

In its complaint, the Commission alleged that between 2017 and 2020, GoodRx, as a vendor of personal health records, disclosed more than 500 consumers' unsecured PHR identifiable health information to third party advertising platforms like Facebook and Google, without the authorization of those consumers. As charged in the complaint, these disclosures violated explicit privacy promises the company made to its users about its data sharing practices (including about its sharing of PHR identifiable health information). The Commission alleged that GoodRx broke these promises and disclosed its users' prescription medications and personal health conditions, personal contact information, and unique advertising and persistent identifiers. The Commission charged GoodRx with violating the Rule by failing to provide the required notifications, as prescribed by the Rule, to (1) individuals whose unsecured PHR identifiable health information was acquired by an unauthorized person, (2) the Federal Trade Commission, and (3) media outlets. 16 CFR 318.3–.6. The Commission entered into a settlement that

---

disclosures and individuals' reasonable expectations. Such authorized uses could include communication of information to the consumer, data processing, or Web design, either in-house or through the use of service providers. Beyond such uses, the Commission expects that vendors of personal health records and PHR related entities would limit the sharing of consumers' information, unless the consumers exercise meaningful choice in consenting to such sharing. Buried disclosures in lengthy privacy policies do not satisfy the standard of 'meaningful choice.'") (citations omitted). 74 FR 42967.

[33] *United States v. GoodRx Holdings, Inc.*, No. 23-cv-460 (N.D. Cal. Feb. 17, 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc*.

imposed injunctive relief and required GoodRx to pay a $1.5 million civil penalty for its alleged violation of the Rule.[34]

Similarly, on May 17, 2023, the Commission brought its second enforcement action under the Rule against Easy Healthcare Corporation ("Easy Healthcare"), a company that publishes an ovulation and period tracking mobile application called Premom, which allows its users to input and track various types of health and other sensitive data. Similar to the conduct alleged against GoodRx, Easy Healthcare disclosed PHR identifiable health information to third party companies such as Google and AppsFlyer, contrary to its privacy promises, and did not comply with the Rule's notification requirements. The Commission entered into a settlement that imposed injunctive relief and required Easy Healthcare to pay a $100,000 civil penalty for its alleged violation of the Rule.[35]

3. Notice of Proposed Rulemaking

Having considered the public comments on the regulatory review notice and its Policy Statement, on June 9, 2023, the Commission issued a Notice of Proposed Rulemaking ("NPRM")[36] proposing to revise the Rule, 16 CFR part 318, in seven ways:

- First, the Commission proposed to revise several definitions in order to clarify the Rule and better explain its application to health apps and similar technologies not covered by HIPAA. Consistent with this objective, the NPRM modified the definition of "PHR identifiable health information" and added two new definitions ("health care provider"

[34] In addition, the Commission alleged that GoodRx's data sharing practices were deceptive and unfair, in violation of Section 5 of the FTC Act.
[35] *United States v. Easy Healthcare Corporation*, No. 1:23-cv-3107 (N.D. Ill. June 22, 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v*.
[36] 88 FR 37819 ("2023 NPRM").

and "health care services or supplies"). These proposed changes were consistent with a number of public comments supporting the Rule's coverage of these technologies.

- Second, the Commission proposed to revise the definition of "breach of security" to clarify that a breach of security includes an unauthorized acquisition of PHR identifiable health information in a personal health record that occurs as a result of a data security breach or an unauthorized disclosure.
- Third, the Commission proposed to revise the definition of "PHR related entity" in two ways. Consistent with its proposal to clarify that the Rule applies to health apps, the Commission first proposed clarifying the definition of "PHR related entity" to make clear that the Rule covers entities that offer products and services through the online services, including mobile applications, of vendors of personal health records. In addition, the Commission proposed revising the definition of "PHR related entity" to provide that entities that access or send unsecured PHR identifiable health information to a personal health record – rather than entities that access or send *any* information to a personal health record – are PHR related entities.
- Fourth, the Commission proposed to clarify what it means for a personal health record to draw PHR identifiable health information from multiple sources.
- Fifth, in response to public comments expressing concern that mailed notice is costly and not consistent with how consumers interact with online technologies like health apps, the Commission proposed to revise the Rule to authorize electronic notice in additional circumstances. Specifically, the proposed Rule adjusted the language in the "method of notice section" and added a new definition of the term "electronic mail." The proposed Rule also required that any notice delivered by electronic mail be "clear and

conspicuous," a newly defined term, which aligns closely with the definition of "clear and conspicuous" codified in the FTC's Financial Privacy Rule.[37]

- Sixth, the Commission proposed to expand the required content of the notice to individuals, to require that consumers whose unsecured PHR identifiable health information has been breached receive additional important information, including information regarding the potential for harm from the breach and protections that the notifying entity is making available to affected consumers. In addition, the proposed Rule included exemplar notices, which entities subject to the Rule could use to notify consumers in terms that are easy to understand.
- Seventh, in response to public comments, the Commission proposed to make a number of changes to improve the Rule's readability. Specifically, the Commission proposed to include explanatory parentheticals for internal cross-references, add statutory citations in relevant places, consolidate notice and timing requirements in single sections, respectively, of the Rule, and add a new section that plainly states the penalties for non-compliance.

The NPRM also included a section discussing several alternatives the Commission considered but did not propose. Although the Commission did not put forth any proposed modifications on those issues, the Commission nonetheless sought public comment on them.

The Commission received approximately 120 comments in response to the NPRM from a wide spectrum of stakeholders, including consumers, consumer groups, trade associations, think

[37] 16 CFR 313.3(b). The FTC's Financial Privacy Rule requires financial institutions to provide particular notices and to comply with certain limitations on disclosure of nonpublic personal information. Using a comprehensive definition of "clear and conspicuous" that is based on the Financial Privacy Rule definition aims to ensure consistency across the Commission's privacy-related rules.

tanks, policy organizations, private sector entities, and members of Congress.[38] As discussed in detail below, commenters addressed the seven topics on which the Commission proposed changes, responded to particular points on which the Commission requested comment, offered additional comment on alternatives that the Commission considered but did not propose, and provided comment on other topics. The majority of commenters expressed support for the Commission's proposed changes.

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, and will ensure that the Rule remains current in the face of changing business practices and technological developments.

II. Analysis of the Final Rule

The following discussion analyzes the amendments to the Rule.

1. Clarification of Entities Covered

a. The Commission's Proposal to Clarify the Entities Covered

The Commission proposed changes to several definitions in § 318.2 to clarify the Rule's application to health apps and similar technologies not covered by HIPAA. First, the proposed Rule revised the definition of "PHR identifiable health information" to remove a cross-reference and instead import language from section 1171(6) of the Social Security Act, 42 U.S.C. 1320d(6), which is also referenced directly in section 13407 of the Recovery Act. The proposed Rule defined "PHR identifiable health information" as information (1) that is provided by or on behalf of the individual; (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; (3) relates

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

to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and (4) is created or received by a health care provider, health plan (as defined in 42 U.S.C. 1320d(5)), employer, or health care clearinghouse (as defined in 42 U.S.C. 1320d(2)).

The Commission explained that this proposed definition covers traditional health information (such as diagnoses or medications), health information derived from consumers' interactions with apps and other online services (such as health information generated from tracking technologies employed on websites or mobile applications or from customized records of website or mobile application interactions), as well as emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases). The Commission sought comment as to whether any further amendment of the definition was needed to clarify the scope of data covered.

Second, the NPRM proposed to define the term "health care provider" that appears in the proposed definition of "PHR identifiable health information" ("is created or received by a health care provider"). The Commission proposed to define this term in a manner similar to the definition of "health care provider" found in 42 U.S.C. 1320d(3) (and referenced in 42 U.S.C. 1320d(6), which is directly referenced in section 13407 of the Recovery Act), to mean a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing health care services or supplies. The Commission observed that this proposed definition, which is consistent with the statutory scheme, differs from, but does not contradict, the definitions or interpretations adopted by HHS.

The Commission sought comment on defining this term more broadly than the term is used in other contexts.

Third, the NPRM proposed to define "health care services or supplies" (the final term in the definition of "health care provider") to include any online service, such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools. The Commission explained that this change clarified that that the Rule applies generally to online services, including websites, apps, and internet-connected devices that provide health care services or supplies, and clarified that the Rule covers online services related not only to medical issues (by including in the definition terms such as "diseases, diagnoses, treatment, medications") but also wellness issues (by including in the definition terms such as "fitness, sleep, and diet").

The Commission explained that these proposed changes to the definitions clarified that developers of health apps and similar technologies providing "health care services or supplies" qualify as "health care providers," such that any individually identifiable health information these products collect or use would constitute "PHR identifiable health information" covered by the Rule. The Commission explained that these proposed changes further clarified that a mobile health application can be a "personal health record" covered by the Rule and the developers of such applications can be "vendors of personal health records."

b. Public Comments Received Regarding the Commission's Proposal to Clarify the Entities Covered

The Commission received numerous comments on the application of the Rule to health apps and similar technologies. A substantial number of commenters supported the Rule's application to health apps and similar technologies not covered by HIPAA as necessary in light of the explosion of health apps and the associated dangers to the privacy and security of consumers' health information.[39] Notably, support for the Commission's proposals came from a variety of commenters—industry associations,[40] businesses,[41] members of Congress,[42] consumer or patient advocacy groups,[43] individual consumers,[44] and anonymous sources.[45] Many commenters argued that safeguards for non-HIPAA covered health data are essential,[46] particularly because consumers generally are not aware of varying legal protections for health

[39] *See generally*, Am. Acad. of Fam. Physicians ("AAFP"); AHIP; AHIMA; Ass'n of Health Info. Outsourcing Serv.'s ("AHIOS"); AMA; Am. Med. Informatics Ass'n ("AMIA"); ANI; Anonymous 1; Anonymous 2; Anonymous 3; Anonymous 4; Anonymous 9; Anonymous 10; Anonymous 11 ; Anonymous 14; Am. Osteopathic Ass'n ("AOA"); Ella Balasa; Beth Barnett; Lauren Batchelor; Bipartisan Pol'y Ctr. ("BPC"); Alan Brewington; Ctr. for Democracy & Tech. ("CDT"); Ctr. for Digit. Democracy ("CDD"); Confidentiality Coal.; Consumer Rep.'s; Elec. Frontier Found. ("EFF"); Elec. Priv. Info. Ctr. ("EPIC"); Dave K.; Members of the House of Representatives; MRO Corp. ("MRO"); Omada Health; Pharmed Out; Planned Parenthood Federation of Amer. ("Planned Parenthood"); CB Sanders; Robb Streicher; SYNGAP1 Foundation and SYNGAP1 Foundation 2; Devin Thompson; Janice Tufte; Michael Turner; U.S. Public Interest Research Group ("U.S. PIRG"); UL Sol.'s; Grace Vinton; WEDI; Anli Zhou. Some commenters elaborated on the nature of the risks to consumers' health data and on the importance to consumers. Two commenters, for example, described research they had performed regarding mental health and/or reproductive health apps' disclosure of consumers' health data to third parties. Mozilla at 3-4; Consumer Reports at 2. Another commenter, a public interest group and advocacy organization, attached a petition containing 9,659 signatures asking for strong rules to protect digital health privacy. US PIRG at 5-230.

[40] *E.g.*, AAFP, AHIMA, AHIOS, AMA, AMIA, AOA; Network Advert. Initiative ("NAI").

[41] *E.g.*, Mozilla; MRO; Omada Health; UL Sol.'s.

[42] *See* Members of the House of Representatives (six members of Congress expressing support for the proposed changes).

[43] *E.g.*, CDD; CDT; EFF; U.S. PIRG.

[44] Ella Balasa; Beth Barnett; Lauren Batchelor; Alan Brewington; Sean Castillo; Dave K.; CB Sanders; Robb Streicher; Devin Thompson; Janice Tufte; Michael Turner; Grace Vinton; Anli Zhou.

[45] Anonymous 1; Anonymous 2; Anonymous 3; Anonymous 4; Anonymous 5; Anonymous 6; Anonymous 9; Anonymous 10; Anonymous 11; Anonymous 14.

[46] *See, e.g.*, AAFP at 1-2; AHIMA at 2; AHIOS at 2; Anonymous 5 at 1; AOA at 1; Am. Speech-Language-Hearing Ass'n ("ASHA") at 1; Am. Psychiatric Ass'n ("APA") at 1; CDT at 3-4; CHIME at 2; EFF at 1; Generation Patient at 1; HIMSS at 2; HIMSS Elec. Health Rec. Ass'n ("HIMSS EHR Ass'n") at 1; MRO at 1-2; Omada Health at 2; PharmedOut at 1; Planned Parenthood at 2-3; Michael Turner at 1; WEDI at 1-4.

data.[47] Indeed, according to some commenters, requiring notification to consumers of the breach of health information not protected by HIPAA is precisely what Congress intended by authorizing the FTC to issue this Rule; the Commission's proposed changes are, therefore, consistent with the goals of the Recovery Act.[48] Some commenters argued that federal privacy legislation is needed to protect non-HIPAA covered health data, but, in the interim, the Commission should strengthen its Rule to protect consumer health data to the extent possible.[49] Other commenters urged the Commission to take even broader measures in this Rule, such as imposing breach prevention measures,[50] banning health-based surveillance technologies or targeted advertising,[51] banning selling or sharing of health data not necessary to provide patient care or mandating data retention limits and deletion,[52] or requiring adherence to standardized terms of service with strong privacy protections.[53]

Although many commenters expressed support for the proposed changes, several business coalitions, industry associations and individual firms opposed the changes, which, they argued, are inconsistent with Congress's intent in the Recovery Act to address a narrow subset of

[47] AHIMA at 2; Anonymous 5 at 1; ASHA at 1; EFF at 1; WEDI at 2. One commenter, a software company that assists digital health companies with legal compliance, argued that three factors, in particular, support greater protection for digital health data: (1) consumers mistakenly believe HIPAA covers all health data; (2) there is a culture within some digital health companies that favors rapid adoption of products to secure venture capital even when compliance infrastructure is lacking; and (3) digital health products deal with sensitive data and inherently present a greater privacy risk given their heavy reliance on data and data exchange compared to traditional medicine. Tranquil Data at 1.

[48] Confidentiality Coal. at 2; Consumer Rep.'s at 4.

[49] *See, e.g.*, AAFP at 2. One commenter, an industry coalition focused on health IT and health care information exchange, emphasized a significant privacy problem adjacent to the Rule: whether HIPAA covered entities should warn patients about the privacy risks associated with health apps and what the federal government can do to apply equal privacy protections to health data, notwithstanding HIPAA's limitations. *See* WEDI at 3. One commenter supported the proposed changes but argued that the Commission should work with Congress to update antiquated terms like "personal health record." HIMSS at 3.

[50] Ella Balasa at 2; PharmedOut at 1.

[51] Light Collective at 5.

[52] EFF at 2.

[53] Texas Med. Ass'n ("TMA") at 1-2.

"personal health records" and therefore exceed the FTC's statutory authority.[54] According to some comments, Congress should address any privacy issues that exceed the narrow scope of the Recovery Act. These commenters also contend that if the Commission believes there has been a violation of Section 5, then the Commission needs to engage in an FTC Act Section 18 rulemaking.[55] One commenter argued further that consumers have different privacy expectations for an electronic health record offered by their physician versus a fitness app (for example) that they download themselves, and the Commission's Rule should respect those differing expectations.[56]

Some commenters opposed to the changes also argued that the revised definitions would reduce choice and access in the marketplace,[57] stifle innovation,[58] or create disincentives for advertising[59] because (1) firms would risk initiating breaches by sharing user data with their partners and (2) in accepting data from health apps, partners such as advertising and analytics firms would risk being covered by the Rule.[60] According to some commenters, placing such strictures on the advertising and service provider ecosystem would raise prices (by, for example, undermining ad-supported services) and thereby harm competition.[61] One commenter argued that while robust protections for consumer health data are needed, the Rule should not be a vehicle for such protections, because it will result in over-notification of consumers (who have

[54] *See, e.g.*, Ass'n of Nat'l Advertisers, Inc. ("ANA") at 4-5; Comput. & Commc'n's Indus. Ass'n ("CCIA") at 2-3; Chamber of Com. ("Chamber") at 1-3; CHI at 2; Consumer Tech. Ass'n ("CTA") at 2; Lab'y Access and Benefits Coal. ("LAB") at 1; Priv. for Am. at 1-2; TechNet at 2.
[55] Priv. for Am. at 2-3; Chamber at 6-7; Health Innovation All. ("HIA") at 1. *See also* Advanced Med. Tech. Ass'n ("AdvaMed") at 1 (recommending that the Commission adopt a privacy framework pursuant to the Advanced Notice of Proposed Rulemaking R111004: Commercial Surveillance and Data Security).
[56] CCIA at 4.
[57] Am. Telemedicine Ass'n ("ATA Action") at 1.
[58] TechNet at 1-2; CTA at 5.
[59] ANA at 3.
[60] Priv. for Am. at 3.
[61] *E.g.*, ANA at 3; Priv. for Am. at 1, 3-4.

largely learned to disregard breach notices) and be a barrier to legislative change on privacy and data security issues more generally.[62] Another commenter argued against a breach notification rule altogether, asserting that the Commission should instead focus on requiring robust data security practices to prevent breaches in the first instance.[63]

Some commenters specifically addressed the proposed changes to the definitions of "PHR identifiable health information" and the new definitions of "health care provider" and "health care services or supplies." First, a number of comments addressed the scope of "PHR identifiable health information." Some commenters urged greater breadth, arguing, for example, that the definition of "PHR identifiable health information" should be expanded to include other types of data, such as data *about* an individual – not just data provided *by or on behalf of* an individual.[64] Other commenters urged the Commission to state expressly that its definition encompasses particular types of information, such as unique persistent identifiers[65] or information about sexual health[66] or substance use or treatment.[67] By contrast, some commenters urged the Commission to narrow the definition or otherwise clarify its limits, by, for example, exempting data relating to clinical research or trials[68] or data that has been de-identified.[69]

Relatedly, some commenters urged the Commission to create a definition of or standard for "identifiable data," "de-identification" or "de-identified data,"[70] such as by adopting HHS's

[62] World Priv F. ("WPF") at 4.
[63] HIA at 2.
[64] Consumer Rep.'s at 3.
[65] *Id.*
[66] BPC at 1-2; Planned Parenthood at 5.
[67] Legal Action Ctr. & Opioid Pol'y Inst. at 1-2.
[68] Soc'y for Clinical Rsch. Sites ("SCRS") at 1.
[69] Future of Priv. F. ("FPF") at 3.
[70] SCRS at 2; Chamber at 7; EPIC at 7-9; FPF at 3-4, LAB at 2; MRO at 4; Network for Pub. Health L. and Texas A&M Univ. ("Network") at 3.

de-identification standard,[71] or by stating that information is identifiable if it is "reasonably linkable to an identified or identifiable individual."[72] Commenters argued that clarifying what constitutes "identifiable" data is necessary both because of the increasing ability for de-identified data to be re-identified[73] and because the market needs clarity to enable uninhibited flow of de-identified health data for research, public health, and commercial activities.[74] Indeed, according to one commenter, failure to clarify the standard could complicate or chill public health research and other innovation.[75] One commenter argued that an objective standard of "reasonable linkability" is better than what the commenter described as the Rule's knowledge-based standard (i.e., whether the company has a reasonable basis to *believe* it can be used to identify an individual).[76] One commenter urged the Commission to issue a new Notice of Proposed Rulemaking on the issue of de-identification alone.[77]

Second, many commenters specifically addressed the Commission's proposed new definition of "health care provider." One commenter applauded the Commission's revised definition of "health care provider," arguing that taking a crabbed view of that or related terms would lead to further fragmentation of health data, which is already fragmented by HIPAA's limited purview.[78] Another commenter noted that the Commission's definition of "health care provider" is simply a logical outgrowth of how consumers interact with health apps: consumers

[71] LAB at 2; Network at 3; SCRS at 2.
[72] FPF at 3.
[73] SCRS at 2.
[74] FPF at 3; Network at 3-4.
[75] Network at 3.
[76] FPF at 3.
[77] Chamber at 7.
[78] CDT at 11.

look to health apps to provide health-related services — the quintessential function of a health care provider.[79]

Other commenters, however, raised concerns that the proposed definition of "health care provider" is confusing in its departure from HIPAA's terminology or is otherwise overbroad.[80] Some commenters argued that this departure from the traditional meaning of the term is not what Congress intended.[81] A few commenters suggested reducing the confusion with the traditional term by re-naming the definition. These commenters suggested that the Commission instead use one of the following terms: "non-HIPAA-regulated health care provider,"[82] "PHR provider,"[83] "Health-related vendor,"[84] "HIPAA covered entity,"[85] or "health-related service provider."[86] Another commenter recommended eliminating the confusion by stating within the definition that it excludes HIPAA-covered entities and their business associates.[87] Another commenter urged the Commission to affirm that its definition would have no impact on the term "health care provider" as used in other regulations.[88]

Several comments also expressed concern with the final phrase of the definition of "health care provider" ("any other entity furnishing health care services or supplies"), as overly broad and confusing. Commenters argued that its breadth (and the breadth of the accompanying definition of "health care services or supplies") would have perverse results, turning retailers of

[79] Confidentiality Coal. at 3-4.
[80] AAFP at 2-3; AdvaMed at 3-4; AHIP at 2; AMA at 2-3; ATA Action at 1; CARIN Alliance at 2-3; CCIA at 3; CTA at 4, 6-9; Datavant at 2; Invitae Corp. ("Invitae") at 4; NAI at 3-4; Software & Info. Indus. Ass'n ("SIIA") at 1-2; TechNet at 2; TMA at 2-3; WPF at 7.
[81] ANA at 5; ATA Action at 1; Invitae at 4-5; Priv. for Am. at 4.
[82] Planned Parenthood at 6.
[83] WPF at 7.
[84] AHIP at 2.
[85] AMA at 3.
[86] AHIP at 2.
[87] Datavant at 2.
[88] AAFP at 2-3.

tennis shoes, shampoo, or vitamins into entities covered by the Rule, which is not what Congress intended.[89] Moreover, it would result not only in compliance burdens for companies (with the downstream effect of raising prices for consumers) but also in massive over-notification of consumers, who will become desensitized to the onslaught of notices.[90]

Several commenters urged the Commission to address this problem by dropping the phrase "any other entity furnishing health care services or supplies" entirely — or at least excising the word "supplies" — from the definition of "health care provider."[91] One commenter recommended replacing the phrase with a different phrase: "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[92] Another commenter recommended expressly excluding retailers.[93] Commenters requested further clarification of certain terms within the definition of "health care provider," including the terms "furnishing"[94] and "health care."[95] And another commenter argued that a better approach would be to jettison the definitions of "health care provider" and "health care services and supplies" entirely and instead apply the Rule to any entity that "promotes its offering as addressing, improving, tracking or informing matters about a consumer's health."[96]

Third, some commenters addressed the proposed definition of "health care services or supplies."[97] Several commenters requested more clarity as to what constitutes an "online

[89] ANA at 7-8; CCIA at 4; CHI at 3-4; CTA at 7-8; SIIA at 2.
[90] ANA at 3; SIIA at 1.
[91] AdvaMed at 4; CHI at 4; CTA at 9; TechNet at 2.
[92] AdvaMed at 4.
[93] CTA at 8-9.
[94] EPIC at 2.
[95] AdvaMed at 3 (urging the Commission to define "health care" and "health care provider" as in 45 CFR 160.103).
[96] WPF at 10.
[97] AdvaMed at 3; AAFP at 3; AHIP at 3; Priv. for Am. at 6-7.

service,"[98] as nearly all commercial activities have some online presence.[99] Several commenters recommended deleting the final phrase of the definition ("or that provides other health-related services or tools") to limit the definition's breadth.[100] Conversely, some commenters urged the Commission to reinforce its breadth, by expressly stating that "health care services or supplies" include services related to "wellness"[101] or to specific health conditions, such as substance abuse disorder diagnosis, treatment, medication, recurrence of use ("relapse") and recovery.[102]

c. The Commission Adopts the Proposed Changes to Clarify the Entities Covered

After considering the comments received, the Commission adopts the proposed changes to the Rule (with only non-substantive, organizational improvements noted below) to clarify that the Rule applies to mobile health applications and similar technologies. The Commission agrees with the substantial number of comments, from many different types of entities and individuals, who argued that such clarification is necessary in light of changing technology (i.e., the mass adoption of health apps) and the privacy and data security risks to consumer health data collected by that technology. The Commission also agrees with commenters who argued that the proposed changes to the Rule are consistent with the Recovery Act, which was intended to bolster breach notifications for consumer health data that falls outside HIPAA. Although the Commission agrees with commenters who argue that consumer health data should enjoy substantial and unfragmented privacy protections, this Rule addresses breach notification, not omnibus privacy protections. While this rulemaking does not address omnibus privacy protections, the Commission observes that companies collecting or holding consumers' sensitive health data

[98] MRO at 2; WPF at 7-8.
[99] WPF at 8.
[100] NAI at 4.
[101] EPIC at 4.
[102] Legal Action Ctr. & Opioid Pol'y Inst. at 3.

should engage in many of the practices commenters described, such as imposing data retention limits, enabling deletion options, and preventing breaches through robust privacy and data security practices.[103]

The Commission is not persuaded that applying the Rule to health apps and similar technologies will have deleterious consequences for individual firms or competition or result in over-notification of consumers. Importantly, the only obligation the Rule imposes is to notify the Commission, consumers, and, in some cases, the media of a breach of unsecured PHR identifiable health information. As noted in the NPRM, many state laws already impose similar, or significantly broader, data breach obligations.[104] Moreover, firms can avoid notification costs entirely by avoiding breaches – by reducing the amount of unsecured PHR identifiable health information they access and maintain (which can be achieved by securing PHR identifiable health information), by de-identifying health information, and by implementing other privacy and data security measures appropriate to the sensitivity of the data. Congress intended for consumers to learn of breaches of their unsecured PHR identifiable health information that fall outside HIPAA; the changes to the Rule help ensure that consumers will receive the notification Congress intended.

The Commission carefully considered the arguments commenters raised that the definitional changes depart from the language or spirit of the Recovery Act. The Commission does not agree. The definitions hew closely to the language of the Recovery Act and to the

[103] In the 2009 Final Rule, the Commission similarly underscored the importance of maintaining protections for health information, stating: "In addition, as noted in the NPRM, the Commission expects entities that collect and store unsecured PHR identifiable health information to maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner." 74 FR at 42971 n.93 (2009).
[104] 88 FR 37832 n.103.

definitions directly referenced by the Recovery Act in section 1171(6) of the Social Security Act, 42 U.S.C. 1320d(6). As many commenters noted, while health apps did not exist when Congress passed the Recovery Act, they function in a similar manner to the personal health records that existed at the time.

For these reasons, the Commission is adopting the proposed definitions, with minor clarifications. First, the Commission has retained the definition of "PHR identifiable health information" as set out in the NPRM, with non-substantive organizational changes noted below. In response to comments that the definition of "PHR identifiable health information" should be broader, the Commission notes that the definition, which closely follows the statutory language, already encompasses most of the categories of data that commenters identified. For example, unique, persistent identifiers (such as unique device and mobile advertising identifiers), when combined with health information, constitute "PHR identifiable health information," if these identifiers can be used to identify or re-identify an individual. Moreover, "PHR identifiable health information" encompasses information about sexual health and substance abuse disorders, because the information "relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual." The Recovery Act states that PHR identifiable health information is information provided "by or on behalf of the individual," so the Commission declines to change this phrase to "about," as one commenter suggested.[105] The Commission notes, however, that information provided "by or on behalf of the individual" will encompass much information "about" an individual, as the consumer is the original source

[105] Consumer Rep.'s at 4.

of most data; many inferences "about" the individual originate from information provided "by or on behalf of the individual."

The Commission does not agree with commenters who sought to narrow the definition of PHR identifiable health information out of concern for the Rule's overall breadth. The Commission notes that liability under the Rule does not arise from a single definition. While data used for public health research, for example, may, in some instances, meet the definition of "PHR identifiable health information," the firm using that data is subject to the Rule only if other conditions are met (i.e., the firm is an entity covered by the Rule).

The Commission declines to create a new definition of "de-identified data" or another similar term, because the definition of de-identification is already embedded in the second part of the definition of PHR identifiable health information ("that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual"). Where there is no "reasonable basis to believe that the information can be used to identify the individual," the information is not identifiable; rather, it is de-identified. If data has been de-identified according to standards set forth by HHS, then there is not a "reasonable basis to believe that the information can be used to identify the individual," as the definition of PHR identifiable health information requires. Because the Commission's standard is consistent with HHS's, the Commission's Rule poses no impediment to health-related research or other flows of de-identified data. The Commission does not view the existing language as a subjective standard that turns on a company's knowledge, as one commenter suggested; by requiring a "*reasonable basis* to believe" that the information is not identifiable, the Rule creates an objective standard. Whether such reasonable basis exists will depend on whether the data can reasonably be linked to an individual consumer. There is no need for a supplemental Notice of

Proposed Rulemaking on this issue, as the Commission is not changing this aspect of the Rule, which closely follows the statute.[106]

Second, the Commission is modifying the proposed definition of "health care provider" to "covered health care provider" to distinguish that term from interpretations of the term "health care provider" in other contexts, which may be more limited in scope. As commenters requested, the Commission affirms that its definition of "covered health care provider" is unique to the Rule; it does not bear on the meaning of "health care provider" as used in other regulations enforced by other government agencies. The Commission adopts this change merely to dispel confusion in terminology; the Commission is not making any substantive change from the definition as proposed. The Commission does not need to state expressly, either in this definition or elsewhere, that the Rule's notification requirements do not apply to HIPAA-covered entities and their business associates, as § 318.1 of the Rule already includes this proviso. The Commission declines to remove the phrase "any other entity furnishing health care services or supplies" from the definition of "health care provider," because this phrase is nearly identical to the language that appears in 42 U.S.C. 1320d(3), which is referenced in the definition of individually identifiable health information in 42 U.S.C. 1320d(6), which is in turn referenced in the definition of PHR identifiable health information in section 13407(f)(2) of the Recovery Act, 42 U.S.C. 17937.[107] The Commission declines to define the terms "furnish" and "health care" as the Commission believes the plain meaning of the term "furnish" (to supply someone with something) is already clear and adding a definition of "health care" is unnecessary in light of the definition of "covered health care provider" and "health care services and supplies." Differences

[106] 42 U.S.C. 17937(f)(2).

[107] The definition of "health care provider" in § 318.2(f) substitutes "entity" for "person" – i.e., "any other entity furnishing health care services or supplies" – because the rest of the Rule speaks in terms of "entities," but the definition in § 318.2(f) is otherwise identical to the statutory definition in 42 U.S.C. 1320d(3).

from HHS's regulations pursuant to HIPAA are appropriate, as the Recovery Act differs from HIPAA, and the Recovery Act's mandate is specifically to cover entities *not* covered by HIPAA.

Third, the Commission is adopting the proposed definition of "health care services or supplies," with one minor modification: the Commission has substituted the word "means" for "includes" to avoid implying greater breadth than the Commission intends. The Commission adopts this change merely to dispel confusion about undue breadth; the Commission does not intend any substantive change from the definition proposed. The Commission otherwise affirms the proposed definition without change. The Commission believes that the term "online service" in the definition of "health care services or supplies" is sufficiently clear because of the examples of "online services" given within the definition itself: website, mobile application, or internet-connected device. Providing an exhaustive list of what constitutes an online service would prevent the definition from being sufficiently flexible to account for future innovation in types of online services. The Commission also retains the catch-all "or that provides other health-related services or tools" for the same reason: to ensure that the Rule's language can accommodate future changes in technology. There is no undue breadth, because that phrase's meaning is in the context of the preceding phrase ("provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet").

In response to some commenters' concerns that the proposed Rule's definition of "health care provider" and "health care services or supplies" would impermissibly cause the Rule to cover retailers of general-purpose items like tennis shoes, shampoo, or vitamins, the Commission disagrees that this would necessarily be the case. A threshold inquiry under the Rule is whether an entity is a "vendor of personal health records," which the Recovery Act defines as "an entity .

. . that offers or maintains a personal health record."[108] The Recovery Act usage of the term "vendor of" in connection with "personal health records" underscores that entities that are not in the business of offering or maintaining (e.g., selling, marketing, providing, or promoting) a health-related product or service are not covered – in other words, they are not "vendors" of personal health records. Thus, to be a vendor of personal health records under the Rule, an app, website, or online service must provide an offering that relates more than tangentially to health.[109]

The Commission notes that a general retailer (one that sells food products, children's toys, garden supplies, healthcare products (such as pregnancy tests), or apparel (such as maternity clothes)) offering consumers an app to purchase and access purchases of these products – by itself – would not make the retailer a vendor of personal health records. In this scenario, purchase information relating to certain items – such as a pregnancy test or maternity clothes from a retailer – may reveal information about that person's health. While this purchase information may be PHR identifiable health information, the retailer in this scenario is not a vendor of personal health records because the app is only tangentially related to health. The Commission notes, however, that there may be scenarios where a general-purpose retailer described above may become a vendor of personal health records under the Rule, such as where the retailer offers an app with features or functionalities that are sold, marketed, or promoted as more than tangentially relating to health.

---

[108] 42 U.S.C. 17921(18); *see also* 42 U.S.C. 17937.

[109] At least one commenter urged a somewhat similar interpretation, contending that a relevant inquiry in determining whether a service offers a personal health record is "the terms under which a product or service is offered to consumers. If an entity promotes its offering as addressing, improving, tracking, or informing matters about a consumer's health, then that entity's offering would be subject to the rule. Thus, any product or services that tracks or addresses physical activity, blood pressure, heart rate, digestion, strength, genetics, sleep, weight, allergies, pain, and similar characteristics would be subject to a PHR rule." *See* WPF at 10.

In addition, the Commission reiterates that a personal health record must be an electronic record of PHR identifiable health information on an individual, must have the technical capacity to draw information from multiple sources, and must be managed, shared, and controlled by or primarily for the individual. The Commission also notes that purchases of items at a brick and mortar retailer where there is no app, website, or online service to access or track that purchase information electronically is not a personal health record, because there is no electronic record at issue. Contrary to the assertions of some commenters, these definitions do not result in undue breadth, because they do not function in isolation. The Commission provides the following examples to illustrate the interplay of these definitions with the definition of "personal health record":

- **Example 1:** Health Advice App or Website A, which is not covered by HIPAA, provides information to consumers about various medical conditions. Its function is purely informational; it does not provide any mechanism through which the consumer may track or record information. Health Advice App or Website A is not a personal health record, because it is not an electronic *record* of PHR identifiable health information on an individual.
- **Example 2:** Health Advice App or Website B, which is not covered by HIPAA, provides information to consumers about various medical conditions *and* provides a symptom tracker, available to consumers who log into the site with a username and password, in which consumers may input symptoms and receive potential diagnoses. Health Advice App or Website B is an electronic record of PHR identifiable health information on an individual, because its information is provided by the individual, it identifies the individual (via username and password), it relates to the individual's health conditions

(the symptoms), and is received by a health care provider (i.e., the entity providing the site itself, as that entity is furnishing the health care service of an online service that provides mechanisms to track symptoms). However, Health Advice App or Website B is not a personal health record to the extent the site does not have the technical capacity to draw information from multiple sources (i.e., if the consumer is its only source of information).

- **Example 3:** Health Advice Website C, which is not covered by HIPAA, functions in the same way as Health Advice App or Website B, except that it collects geolocation data via an application programming interface ("API"). For the reasons stated in Example 2, it is an electronic record of PHR identifiable health information on an individual. It also has the technical capacity to draw information from multiple sources (consumer inputs and collection of geolocation data through the API. It is managed primarily for the individual (i.e., to provide the individual health advice). Therefore, Health Advice App or Website C is a personal health record.
- **Example 4:** Health Advice App or Website D, which is not covered by HIPAA, functions in the same way as Health Advice App or Website B, except that it also draws information from a data broker and connects that information to some of its individual users to provide them with more accurate diagnostic suggestions. For the reasons stated in Example 2, it is an electronic record of PHR identifiable health information on an individual. It also has the technical capacity to draw information from multiple sources (the consumer and the data broker) and is managed by or primarily for the individual. Therefore, Health Advice App or Website D is a personal health record.

Whether a health app or other electronic record constitutes a personal health record (and is therefore subject to the Rule) is a fact-intensive inquiry whose outcome depends not only on the nature of the information contained in that record, but also on numerous other factors, such as its "technical capacity," its source(s) of information, and its relationship to the individual.

Finally, the Commission notes a non-substantive, organizational change relating to the definition of "PHR identifiable health information." In the 2023 NPRM, the Commission proposed revising "PHR identifiable health information" by importing language from section 1171(6) of the Social Security Act, 42 U.S.C. 1320d(6), which is referenced directly in section 13407 of the Recovery Act. To hew more closely to the organization of the Recovery Act, and to preserve the word "includes" in the phrase "includes information that is provided by or on behalf of the individual," the Commission revised slightly the order of the elements in the definition of "PHR identifiable health information."

2. Clarification of What it Means for a Personal Health Record to Draw Information from Multiple Sources

a. The Commission's Proposal Regarding What It Means for a Personal Health Record to Draw Information from Multiple Sources

The Commission proposed amending the definition of the term "personal health record" to clarify what it means for a personal health record to draw information from multiple sources. Under the 2009 Rule, a personal health record is defined as an electronic record of PHR identifiable health information that *can be drawn* from multiple sources and that is managed, shared, and controlled by or primarily for the individual. [italics added]. Under the Commission's proposed definition, a "personal health record" would be defined as an electronic record of PHR identifiable health information on an individual that has the *technical capacity* to

draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual. [italics added].

Changing the phrase "that can be drawn from multiple sources" to "has the technical capacity to draw information from multiple sources" serves several purposes. First, it clarifies that a product is a personal health record if it can draw information from multiple sources, even if the consumer elects to limit information to a single source only, in a particular instance. For example, a depression management app that accepts consumer inputs of mental health states and has the technical capacity to sync with a wearable sleep monitor is a personal health record, even if some customers choose not to sync a sleep monitor with the app. Thus, whether an app qualifies as a personal health record would not depend on the prevalence of consumers' *use* of a particular app feature, like sleep monitor-syncing. Instead, the analysis of the Rule's application would be straightforward: either the app has the technical means (e.g., the application programming interface or API) to draw information from multiple sources, or it does not. Next, adding the phrase "technical capacity to draw information" clarifies that a product is a personal health record if it can draw *any* information from multiple sources, even if it only draws *health* information from one source. This change further clarifies the Commission's interpretation of the Recovery Act, as explained in the Policy Statement.[110]

The Commission sought public comment as to whether this revised language sufficiently clarifies the Rule's application to developers and purveyors of products that have the technical capacity to draw information from more than one source. The Commission invited comment on its interpretation that an app is a personal health record because it has the technical capacity to draw information from multiple sources, even if particular users of the app choose not to enable

[110] Policy Statement at 2.

the syncing features. The Commission also requested comment about whether an app (or other product) should be considered a personal health record even if it only draws *health* information from one place (in addition to non-health information drawn elsewhere); or only draws *identifiable* health information from one place (in addition to non-identifiable health information drawn elsewhere). The Commission further requested comment about whether the Commission's bright-line rule (apps with the "technical capacity to draw information" are covered) should be adjusted to take into account consumer use, such as where no consumers (or only a de minimis number) use a feature, and about the likelihood of such scenarios. For example, the Commission offered an example of an app that might have the technical capacity to draw information from multiple sources, but its API is entirely or mostly unused, either because it remains a Beta feature, has not been publicized, or is not popular.

b. Public Comments Regarding What It Means for a Personal Health Record to Draw Information from Multiple Sources

Many commenters supported the Commission's proposal amending the definition of a "personal health record."[111] Commenters noted that, for instance, this change would help to ensure that many services that collect PHR identifiable health information are covered by the Commission's Rule,[112] and would help to promote greater privacy and security for health information,[113] while still "hewing to the limitations of the statute."[114] Some commenters noted that without this change, developers of personal health records (such as app developers) might have incentives to design their products in ways that would intentionally skirt the Rule's

[111] Ella Balasa at 1; TMA at 4 (arguing that "PHRs include applications with the technical capacity to draw information from multiple sources, regardless of the patient's preference to activate the technical capability."); Consumer Rep.'s at 6; AAFP at 3; AHIMA at 4–5; AMA at 4; CHIME at 4; CDT at 13; AOA at 3.
[112] AHIMA at 4–5.
[113] AAFP at 3.
[114] Consumer Reports at 5–6.

requirements (such as by restricting a consumer's ability to import data from other sources).[115] Others noted the importance of the Rule covering apps with the technical capacity to draw information from multiple sources even where such capacity is not used by the consumer.[116]

Other commenters opposed this proposal.[117] Some argued that the proposed clarification regarding what drawing information from multiple sources means runs counter to Congress's statutory intent,[118] because virtually every app has some sort of integration (e.g., for analytics) through which it draws information other than from the consumer.[119] One commenter asserted that the change would broaden the scope of the Rule to the point that it would sweep in online services that should not be thought of as a personal health record (such as email apps),[120] or otherwise create confusing standards for app developers or reduce innovation.[121] In addition, commenters expressed concern that this change would sweep in apps or online services that have the technical capacity to draw from multiple sources during the development or testing phase of the product, or that would sweep in products with unused, unavailable, or unpublicized APIs or integrations that count as a source.[122] One commenter expressed concern about lack of clarity,

---

[115] AHIP at 2–3; CDT at 13 (arguing that changes remove "incentives for companies to technically design products and services to not trigger the HBNR to avoid any need to provide consumer notice.").
[116] AHIOS at 4; CARIN Alliance at 4.
[117] NAI at 6 (urging that the Commission make clear that a personal health record is one that "not only has the technical capacity to draw PHR identifiable health information from multiple sources, but that it also has the functionality and actually does incorporate data from multiple sources."); ANA at 7; ACLA at 1–2.
[118] NAI at 6.
[119] Chamber at 4-5; Priv. for Am. at 5-6; NAI at 6.
[120] CCIA at 6.
[121] CTA at 11; AdvaMed at 5; CHI at 5.
[122] CHI at 5 (asking the Commission to clarify that an "app having the ability to draw from multiple sources with some changes to the app's coding/APIs is not within this definition's threshold."); ACLA at 1 (arguing that "[i]f a feature is unused by individuals 'because it remains a Beta feature,' then in fact it does not have the 'technical capacity' to draw an individual's information from other sources, unless and until its functionality has been enabled by the vendor. The mere possibility that an application vendor *might* sometime in the future enable that functionality should not bring the electronic record within the scope of the definition of 'personal health record.'") (emphasis in original); CTA at 11 (arguing that Rule should instead have bright-line test that assesses whether the app actually draws health information from multiple sources); AdvaMed at 5 (arguing that the Commission should decline to adopt multiple sources changes because it could cause confusion and potentially sweep in apps or services with features that have not been made available to consumers, such as APIs connected to the PHR that have not been publicized).

such as in scenarios where a user is required to pay for an upgrade to access a feature or integration that draws information from another source.[123] Some commenters also expressed concern that apps and online services that are subject to HIPAA (i.e., HIPAA-covered entities or business associates) should be carved out of the definition of a personal health record.[124] Other commenters expressed broader concern with the definition of "personal health record," urging the Commission to, for example, abandon the purportedly outdated term in favor of a more modern one.[125] For instance, some commenters urged that the Commission abandon or tweak the requirement that the personal health record be "managed, shared, and controlled by or primarily for the individual."[126]

Another commenter expressed concern that the proposed change could sweep in services that draw any information from multiple sources, regardless of whether that information is identifiable health information.[127]

a. The Commission Adopts the Proposed Changes Clarifying What It Means for a Personal Health Record to Draw Information from Multiple Sources

After considering the comments received, the Commission adopts the proposed amendment without change. This amendment will help clarify the types of entities covered by the Rule. The definition does not create undue breadth or deviate from Congressional intent; rather, the changes are consistent with the language of the Recovery Act, and only serve to give meaning to the phrase "can be drawn" in the Recovery Act in a way that is consistent with the current state of technology. They are also necessary to keep pace with technological change,

[123] WPF at 9.
[124] Omada at 5; Datavant at 3.
[125] HIMSS at 3 (urging the Commission to work with Congress to craft a definition more consonant with technological realities).
[126] AHIOS at 4; MRO at 4.
[127] NAI at 6.

which has enabled firms to offer consumers mobile electronic records of their health information that contain numerous integrations. To illustrate the intended meaning of the proposed revisions to the term "personal health record," the Commission reiterates examples from the 2023 NPRM of two non-HIPAA covered diet and fitness apps available for consumer download in an app store. Under the amended Rule, each is a personal health record.

- **Example 1:** Diet and Fitness App Y allows users to sync their app with third-party wearable fitness trackers. Diet and Fitness App Y has the technical capacity to draw identifiable health information both from the user (e.g., name, weight, height, age) and the fitness tracker (e.g., user's name, miles run, heart rate), even if some users elect not to connect the fitness tracker.
- **Example 2:** Diet and Fitness App Y has the ability to pull information from the user's phone calendar via the calendar API to suggest personalized healthy eating options. Diet and Fitness App Y has the technical capacity to draw identifiable health information from the user (e.g., name, weight, height, age) and non-health information (e.g., calendar entry info, location, and time zone) from the user's calendar.

As these examples make clear, and in response to one commenter's concern that the changes would sweep in services that do not draw any health information,[128] the Commission notes that the Rule still requires drawing PHR identifiable health information from at least one source to count as a personal health record.

The Commission declines to make other requested changes to the definition of personal health record. First, the Commission declines to include an express exemption for HIPAA-covered entities within the definition of personal health record because § 318.1 of the Rule

[128] NAI at 6.

already specifically exempts businesses or organizations covered by HIPAA.[129] Second, the Commission declines to exempt apps and services where there are available but unused or unpublicized APIs or integrations. Similarly, the Commission declines to exempt apps and services from the definition just because they are drawing information from multiple sources while undergoing product or beta testing and are not yet in their final form.[130] The Commission notes that a product feature or integration that exists and that is able to draw PHR identifiable health information counts as a source under the Rule. Exempting such instances would be contrary to the purpose of the Rule and would impermissibly limit notification of breaches just because a product feature is not widely disseminated, used, or in its final form. The Commission notes that under the Rule, a covered entity that experienced a breach of security of unsecured PHR identifiable health information triggering the Rule would not be exempt because the breach occurred in the context of such scenarios.

Further, and importantly, the Rule is triggered only by breaches of unsecured PHR identifiable health information and does not apply to information that is protected or "secured" through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009, 42 U.S.C. 17932(h)(2).[131] The Rule, therefore, creates appropriate

[129] *See*, *e.g.*, 16 CFR 318.1 (a) (Rule "does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity."); *see also* 16 CFR 318.2 (f), (j) (exempting business associates and HIPAA-covered entities from the Rule's definitions of "PHR related entity" and "vendor of personal health records.").

[130] ACLA at 1–2; CTA at 11; AdvaMed at 5.

[131] Per HHS guidance, electronic health information is "secured" if it has been encrypted according to certain specifications set forth by HHS, or if the media on which electronic health information has been stored or recorded is destroyed according to HHS specifications. *See* 74 FR 19006; *see also* U.S. Dep't of Health & Human Servs., *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (July 26, 2013), *https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html*. PHR identifiable health information would be considered "secured" if such information is disclosed by, for example, a vendor of personal health records, to a PHR related entity or a third party service provider, in an encrypted format meeting HHS specifications, and the PHR related entity or third party service

incentives for product testing with de-identified data or that secures information through certain specifications, such as through specified encryption methods.

Third, the Commission declines, as one commenter requested,[132] to expressly exempt scenarios where a change is required to an app's coding to draw information from another source. The Commission notes, however, that it does not intend to cover instances where an app can draw from multiple sources only through changes to the design or underlying software code and where the app developer does not implement those changes.

In addition, the Commission declines to remove from the definition of personal health record the requirement that it be "managed, shared, and controlled by or primarily for the individual." This language mirrors the Recovery Act's statutory definition of personal health record.[133] Further, this language provides a boundary to the definition. Even if a website or app has the technical capacity to draw information from multiple sources (for example, because it has integrations for advertising or analytics), it must still be "managed, shared, and controlled by or primarily for the individual" to be covered by the Rule.

Generally, a personal health record is an electronic record of an individual's health information by which the individual maintains access to the information and may have, for example, the ability to manage, track, control, or participate in his or her own health care. If

provider stores the data in an encrypted format that meets HHS specifications and also stores the encryption and/or decryption tools on a device or at a location separate from the data.

[132] CHI at 5 (asking the Commission to clarify that an "app having the ability to draw from multiple sources with some changes to the app's coding/APIs is not within this definition's threshold.").

[133] 42 U.S.C. 17921(11).

these elements are not present, the website or app may not be "managed, shared, and controlled by or primarily for the individual," and would not, therefore, constitute a personal health record.

3. Clarification Regarding Types of Breaches Subject to the Rule

a. The Commission's Proposals

i. The Commission's Proposals Regarding "Breach of Security"

The Commission proposed a definitional change to clarify that a breach of security under the Rule encompasses unauthorized acquisitions that occur as a result of a data breach *or* an unauthorized disclosure. The Commission's proposal underscores that a breach of security is not limited to data exfiltration, and includes unauthorized disclosures (such as, but not limited to, a company's unauthorized sharing or selling of consumers' information to third parties that is inconsistent with the company's representations to consumers). The Rule previously defined "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual, which language mirrored the definition of "breach of security" in section 13407(f)(1) of the Recovery Act.

Accordingly, consistent with the Recovery Act definition, the Policy Statement, FTC enforcement actions under the Rule, and public comments received, the Commission proposed amending the definition of "breach of security" in § 318.2(a) by adding the following sentence to the end of the existing definition: "[a] breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure." The change was intended to make clear to the marketplace that a breach includes an unauthorized acquisition of identifiable health information that occurs as a result of a data breach or an unauthorized disclosure, such as a voluntary disclosure made by the PHR vendor or PHR related entity where such disclosure was not

authorized by the consumer.

The NPRM, like the 2009 Rule, continued to include a rebuttable presumption for unauthorized access to an individual's data; it stated that when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach "has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information."

ii. The Commission's Related Proposal to Not Define the Term "Authorization" in the Rule

In the 2023 NPRM, the Commission stated that it had considered defining the term "authorization," which appears in § 318.2(a)'s definition of "breach of security," but did not propose any such change in the NPRM.

The Commission considered defining "authorization" to mean the affirmative express consent of the individual and then defining "affirmative express consent" consistent with state laws that define consent, such as the California Consumer Privacy Rights Act, Cal. Civ. Code 1798.140(h).[134] Such changes would have ensured that notification is required anytime there is acquisition of unsecured PHR identifiable health information without the individual's affirmative express consent for that acquisition—such as when an app discloses unsecured PHR identifiable health information to another company, having obtained nominal "consent" from the individual

[134] As noted in the 2023 NPRM, the Commission considered defining "affirmative express consent" as follows:

Affirmative express consent means any freely given, specific, informed, and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a clear and conspicuous disclosure to the individual, apart from any "privacy policy," "terms of service," "terms of use," or other similar document, of all information material to the provision of consent. Acceptance of a general or broad terms of use or similar document that contains descriptions of agreement by the individual along with other, unrelated information, does not constitute affirmative express consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute affirmative consent. Likewise, agreement obtained through use of user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, does not constitute affirmative express consent. *See* 88 FR 37830 n.78.

by using a small, greyed-out, pre-selected checkbox following a page of dense legalese.

The Commission did not, however, propose to define "authorization" because (1) the 2009 Rule Commentary already provided guidance on the types of disclosures that the Commission considers to be "unauthorized"[135]; (2) recent Commission orders, such as the Commission's enforcement actions against GoodRx and Easy Healthcare,[136] also make clear that the use of "dark patterns," which have the effect of manipulating or deceiving consumers, including through use of user interfaces designed with the substantial effect of subverting or impairing user autonomy and decision-making, do not satisfy the standard of "meaningful choice"; and (3) Commission settlements establish important guidelines involving authorization (the Commission's recent settlement with GoodRx, alleging violations of the Rule, highlights that disclosures of PHR identifiable health information inconsistent with a company's privacy promises constitute an unauthorized disclosure).

The Commission sought public comment about:

- Whether the commentary above and FTC enforcement actions under the Rule provide sufficient guidance to put companies on notice about their obligations for obtaining consumer authorization for disclosures, or whether defining the term "authorization" would better inform companies of their compliance obligations.

[135] *See*, *e.g.*, 74 FR 42967.
[136] *United States* v. *GoodRx Holdings, Inc.,* No. 23–cv–460 (N.D. Cal. 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc; United States* v. *Easy Healthcare Corp.,* No. 1:23–cv–3107 (N.D. Ill. 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v*.

- To the extent that including such definitions would be appropriate, the definitions of "authorization" and "affirmative express consent," as described above, and the extent to which such definitions are consistent with the language and purpose of the Recovery Act.
- What constitutes an acceptable method of authorization, particularly when unauthorized sharing is occurring.[137]
- Whether there are certain types of sharing for which authorization by consumers is implied because such sharing is expected and/or necessary to provide a service to consumers.

b. Public Comments

i. Public Comments Received Regarding "Breach of Security"

Many commenters supported the Commission's proposed amendment to the definition of "breach of security."[138] One commenter noted that the change is consistent with the broad definition of "breach of security" in the Recovery Act, which refers explicitly to the acquisition of PHR identifiable health information without the authorization of an individual (rather than the authorization of an entity holding the data, as is the case where a breach involves data theft or exfiltration).[139] Commenters also noted that the amendment would ensure notice, accountability, and regulatory oversight, regardless of the underlying cause of the unauthorized acquisition.[140]

[137] For example, the Commission sought comment on the following: "when a vendor of personal health records or a PHR-related entity is sharing information covered by the Rule, is it acceptable for that entity to obtain the individual's authorization to share that information when an individual clicks 'agree' or 'accept' in connection with a pre-checked box disclosing such sharing? Is it sufficient if an individual agrees to terms and conditions disclosing such sharing but that individual is not required to review the terms and conditions? Or is it sufficient if an individual uses a health app that discloses in its privacy policy that such sharing occurs, but the app knows via technical means that the individual never interacts with the privacy policy?" *See* 88 FR 37832.
[138] *See, e.g.*, TMA at 3; U.S. PIRG at 2–3; AAFP at 3; AHIMA at 3; AMA at 3–4; AMIA at 3; AOA at 2–3; AHIOS at 3; CDT at 11–12; CHIME at 4; EPIC at 5–6.
[139] Consumer Rep.'s at 4.
[140] CDT at 11–12; U.S. PIRG at 2–3.

Commenters noted that breaches encompass more than just cybersecurity intrusions.[141] Commenters also argued that a company's voluntary unauthorized disclosure can be just as damaging as data theft.[142] For instance, a commenter noted that unauthorized disclosures of health information may cause embarrassment, perpetuate stigma about patients' conditions, deter patients from seeking care, interfere in the patient-physician relationship, or impact patients' employment.[143] Moreover, voluntary, unauthorized disclosures increase the risk of additional unauthorized acquisition and sharing of this information among bad actors.[144]

Some commenters supported expanding or changing the definition further. Specifically, some commenters urged the Commission to amend the definition to encompass (1) exceeding authorized access or use of PHR identifiable health information, such as where a company collects data for one purpose, but later uses or discloses that data for a second, undisclosed purpose;[145] or (2) the collection or retention of PHR identifiable health information beyond what is necessary to provide the associated service to an individual consumer.[146] One commenter asked the Commission to clarify that the Rule would be triggered by unauthorized use of or access to information derived from PHR identifiable health information, and to define the phrase acquisition.[147]

Some commenters, however, urged the Commission to not amend the definition at all. These commenters expressed concern that the amendment would cause the Rule to exceed what Congress intended in the Recovery Act and transform the Rule into an opt-in notice and consent

[141] AMA at 4; CDT at 11–12; EPIC at 5.
[142] AAFP at 3; CDT at 11–12.
[143] AOA at 2.
[144] AHIMA at 3.
[145] FPF at 12–15.
[146] EPIC at 5–7; U.S. PIRG at 2–3.
[147] Mozilla at 6–7.

privacy regime.[148] Commenters argued further that the proposed changes would cause consumer notice fatigue,[149] consumer panic,[150] or over-reporting by companies.[151] One commenter urged the Commission to limit the definition of "acquisition" to actual acquisition, and exclude instances of access or disclosure where the information was not actually acquired by a third party.[152] Commenters argued that the proposed definition would be burdensome and force companies to limit certain beneficial disclosures to certain third parties, such as disclosures to support internal operations, detect security vulnerabilities or fraud, for law enforcement, and other purposes.[153]

Some commenters also urged that the Commission adopt carve-outs so that certain conduct would not be deemed breaches of security under the Rule. Commenters requested exemptions consistent with or found in HIPAA or under state breach notification laws, such as exemptions for disclosures to certain types of entities or for certain purposes, or where there is inadvertent or unintentional access, use, or disclosure.[154] Commenters also proposed safe

[148] Chamber at 6; Priv. for Am. at 2–5; ANA at 6–7.
[149] SIIA at 3; CTA at 13–14.
[150] CCIA at 4–5, 7 (arguing that requiring notification for unauthorized disclosures could cause consumers to worry in the absence of harm, such as where it is "typical" to disclose such information.)
[151] CTA at 13–14.
[152] *Id.* at 14–16.
[153] TechNet at 3; Chamber at 7; CCIA at 5–6.
[154] CHI at 4 (stating that the FTC "should explicitly except the same situations from disclosure that are excepted from HIPAA disclosures, and/or try to align exceptions with those found in state privacy statutes."); CTA at 16; HIA at 2; TechNet at 3 (arguing that the Rule should adopt exemptions that encompass "actions taken to prevent and detect security incidents, to comply with a civil, criminal, or regulatory inquiry or investigation, to cooperate with law enforcement agencies concerning conduct or activity that the data controller reasonably and in good faith believes may be illegal, to perform internal operations consistent with a consumer's expectations, and to provide a product or service that a consumer requested."); CCIA at 5–6 (arguing that the Rule should exempt disclosures relating to a host of purposes, including: preventing and detecting security incidents and fraud, complying with legal process, cooperating with law enforcement, performing internal operations consistent with consumer expectations, providing a service requested by the consumer, protecting "the vital interests of the consumer," or processing data relating to public health); Chamber at 7 (arguing that if the Commission does amend the definition of breach of security, it "should provide exceptions for legitimate and societally beneficial uses of data that other privacy laws have for failure to honor opt-in including but not limited to network security, prevention and detection of fraud, protection of health, network maintenance, and service/product improvement."); LAB at 2.

harbors for companies that implement recognized security or privacy safeguards;[155] and one commenter proposed safe harbors that would apply where data is shared with "affiliated businesses," where there is inadvertent but "good-faith" access by a company employee, where a company makes good faith efforts to inform consumers of disclosures to third parties, and where companies take steps to contractually limit downstream uses of the data.[156] Other commenters expressed support for exempting disclosures of PHR identifiable health information to public health authorities for public health purposes, noting that the amended definition could discourage such disclosures.[157]

ii. Public Comments Received Regarding Defining "Authorization"

Commenters were divided as to whether the Commission should define "authorization." Some commenters supported defining "authorization" to provide greater guidance to companies, to promote transparency, and to discourage buried or inconspicuous disclosures relating to health information, or approaches to consent that are not meaningful because they are confusing or coercive.[158] To further regulatory consistency, some commenters supported adding a definition of "authorization" that is consistent with how that term is defined in other health-related laws, such as under HIPAA[159] or state health privacy laws that define consent or authorization (such as the California Consumer Privacy Rights Act[160] or the Washington My Health, My Data Act).[161]

---

[155] DirectTrust at 1–2.
[156] ATA Action at 2.
[157] Network for Pub. Health L. and Texas A&M Univ. at 1–2.
[158] AHIP at 4; Light Collective at 4; MRO at 2–3; Mozilla at 4; CARIN Alliance at 10; Consumer Rep.'s at 9; *see also* PharmedOut at 3 (arguing that defining "authorization" is crucial but urging that the Commission go further and place substantive restrictions on what companies can do with consumer health data.).
[159] AdvaMed at 7 (arguing that any definition of "authorization" or "affirmative express consent" should take into account the necessity for medical technologies and medical technology companies to be able to operate and communicate under standards consistent with those governing HIPAA covered entities and others in the health care ecosystem. These standards permit certain uses and disclosures of individually identifiable health information without express consent where necessary for the provision of timely and effective health care); MRO at 3; AHIMA at 7–8.
[160] AHIOS at 3.
[161] Consumer Rep.'s at 9.

By contrast, some commenters opposed defining the term—or opposed a requirement under the Rule that entities be required to get authorization before disclosing PHR identifiable health information.[162] Commenters argued that Congress had not granted the Commission the authority to define "authorization" in the Recovery Act,[163] or that doing so would import a substantive consent requirement that is outside the scope of the Rule, converting a breach notice Rule into an opt-in privacy regime.[164] Other commenters noted that requiring a specifically defined authorization would create an inflexible standard that would not evolve with changes in technology.[165] Other commenters opposed a requirement that consumers should be required to review terms before agreeing to use a service, contending that this would not increase consumer understanding of terms.[166]

Some commenters endorsed other approaches that would exempt from any requirement of affirmative express consent certain types of disclosures of PHR identifiable health information, such as to service providers, data processors, and entities that assist with combatting fraud and promoting safety.[167] Some commenters urged that a disclosure be deemed authorized if the disclosure is consistent with a company's privacy notices or policies or where applicable state privacy laws require affirmative consent or provide for the right to opt-out, without the need to define affirmative express consent under the Rule.[168] One commenter argued that

[162] HIA at 2 (arguing that "[r]outine disclosures of data should be allowed in certain contexts without additional need for authorizations"); CTA at 16–17; AdvaMed at 7–8; ACLA at 6; Confidentiality Coal. at 4–5.
[163] Confidentiality Coal. at 4–5.
[164] CTA at 16–17 (arguing that the Rule does not allow the Commission to impose "substantive consent requirements" that would be burdensome and "likely not administrable for many companies.").
[165] SIIA at 4.
[166] CHI at 7.
[167] FPF at 10 (arguing that "an organization may share information with a service provider operating on their behalf to provide storage; may share information to protect the safety or vital interests of an individual or react to a public health emergency; or to protect themselves against security incidents and fraud. In each of these situations, data protection laws typically invoke a variety of non-consent measures, including data minimization, transparency, notice to the end-user or the regulator, and opportunities to object."); Chamber at 7.
[168] Confidentiality Coal. at 4–5; SIIA at 4; CHI at 7.

authorization should be met when a consumer agrees to opt-in to certain data sharing, such as by clicking a box proximate to a disclosure of material terms.[169]

c. The Commission Adopts the Proposed Changes to the Definition of "Breach of Security"

After carefully considering the public comments, the Commission adopts the proposed amendment without change. The Final Rule definition is consistent with the statutory definition in the Recovery Act, the Policy Statement,[170] and recent Commission enforcement actions under the Rule. The Commission notes that the statutory definition in the Recovery Act is sufficiently broad to cover both cybersecurity intrusions as well as a company's intentional but unauthorized disclosures of consumers' PHR identifiable health information to third party companies. In addition, the Commission finds persuasive the comment noting that the Recovery Act's definition of "breach of security" refers to the acquisition PHR identifiable health information without the authorization of an ***individual***, rather than the authorization of the entity holding the data.[171] The definition is also consistent with public comments received by the Commission in 2020 (when the Commission announced its regular, ten-year review of the Rule and requested public comments about potential Rule changes[172]), which urged the Commission to clarify what constitutes an unauthorized acquisition under the Rule.[173] Importantly, the amendment to the

---

[169] CTA at 17.

[170] The Commission's Policy Statement makes clear that "[i]ncidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule," and that a breach "is not limited to cybersecurity intrusions or nefarious behavior." Policy Statement at 2.

[171] Consumer Rep.'s at 5 (noting that "the Recovery Act frames breaches of security in relation to individuals, rather than to vendors of personal health records or PHR related entities," and defines breach of security as "acquisition of such information without the authorization of the individual.")

[172] 85 FR 31085 (May 22, 2020).

[173] *See* Public Comments in response to May 2020 Request for Public Comments in connection with regular, ten-year review of Rule: AMA at 5–6 ("The FTC should define 'unauthorized access' as presumed when entities fail to disclose to individuals how they access, use, process, and disclose their data and for how long data are retained. Specifically, an entity should disclose to individuals exactly what data elements it is collecting and the purpose for their collection"; "[T]he FTC should define 'unauthorized access' as presumed when an entity fails to disclose to an

definition of "breach of security" in § 318.2(a) does not depart from the 2009 Rule Commentary or the Commission's enforcement policy under the Rule. Instead, it further underscores the 2009 Rule Commentary and subsequent Commission enforcement actions that unauthorized disclosures (i.e., sharing inconsistent with consumer expectations) can be a "breach of security" that triggers the Rule.[174]

The Commission declines to adopt any specific exemptions or safe harbors to the definition of breach of security. Unlike the section of the Recovery Act that governs breach notifications under HIPAA,[175] Congress did not provide for any specific, enumerated exemptions for breaches under the Commission's Rule. Moreover, the Commission's Rule provides for a rebuttable presumption for certain types of access: when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach "has

individual the specific secondary recipients of the individual's data."); AMIA at 2 (recommending that the FTC "[e]xpand on the concept of 'unauthorized access' under the definition of 'Breach of security,' to be presumed when a PHR or PHR related entity fails to adequately disclose to individuals how user data is accessed, processed, used, reused, and disclosed."); OAG–CA at 5–6 (urging the FTC to include "impermissible acquisition, access, use, disclosure" under the definition of breach.). These comments can be found at https://www.regulations.gov/docket/FTC-2020-0045.

[174] The 2009 Rule Commentary noted other examples illustrating that unauthorized sharing or transferring of information constitutes a breach of security, including that the unauthorized downloading or *transfer* of information by an employee can constitute a breach of security; that inadvertent access by an unauthorized employee reading or *sharing* information triggers the Rule's notification obligations; and notes that given the highly personal nature of health information, "the Commission believes that consumers would want to know if such information was read or *shared* without authorization." (emphasis added). *See* 74 FR 42966–67.

[175] 42 U.S.C. 17921; *see also* U.S. Dep't of Health & Human Servs., *Breach Notification* (July 26, 2013), *https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html*. Under the Recovery Act's definition of "breach of security" for the Rule governing HIPAA-covered entities and business associates, the statute explicitly provides for three exceptions: (1) unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority; (2) the inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates; and (3) if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information. *See* 45 CFR 164.400-414. In the first two cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. These exceptions are not found in the provisions of the Recovery Act authorizing the FTC's Health Breach Notification Rule; this makes sense, given that there is no analogous Privacy Rule, Security Rule, or required Business Associate agreements outside the HIPAA sphere governing entities covered by the FTC's Health Breach Notification Rule.

reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." That is, companies can rebut the presumption of acquisition in instances of unauthorized access by providing reliable evidence disproving acquisition. The Commission has previously offered guidance on what counts as unauthorized access and reiterates that guidance here.[176]

d. The Commission Affirms Its Proposal Not to Define "Authorization"

After carefully considering the public comments, the Commission declines to define "authorization," as that term appears in § 318.2(a)'s definition of "breach of security." The Commission finds persuasive the public comments suggesting that imposing an affirmative express consent requirement would not be appropriate or warranted in all cases.

The Commission believes that whether a disclosure is authorized under the Rule is a fact-specific inquiry that will depend on the context of the interactions between the consumer and the company; the nature, recipients, and purposes of those disclosures; the company's representations to consumers; and other applicable laws. The Commission reiterates the 2009 Rule Commentary, which states that a use of data is "authorized" only where it is consistent with

[176] The Rule continues to provide that, when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach "has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." As noted in the 2009 Rule Commentary, "the presumption was intended to address the difficulty of determining whether access to data (i.e., the opportunity to view the data) did or did not lead to acquisition (i.e., the actual viewing or reading of the data). In these situations, the Commission stated that the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has taken place. In describing the rebuttable presumption, the Commission provided several examples. It noted that no breach of security has occurred if an unauthorized employee inadvertently accesses an individual's PHR and logs off without reading, using, or disclosing anything. If the unauthorized employee read the data and/or shared it, however, he or she ''acquired'' the information, thus triggering the notification obligation in the Rule. Similarly, the Commission provided an example of a lost laptop: If an entity's employee loses a laptop in a public place, the information would be accessible to unauthorized persons, giving rise to a presumption that unauthorized acquisition has occurred. The entity can rebut this presumption by showing, for example, that the laptop was recovered, and that forensic analysis revealed that files were never opened, altered, transferred, or otherwise compromised." *See* 74 FR 42966.

a company's disclosures and consumers' reasonable expectations and where there is meaningful choice in consenting to sharing—buried disclosures do not suffice.[177]

The Commission's recent enforcement actions alleging violations of the Rule against GoodRx and Easy Healthcare further highlight that disclosures of PHR identifiable health information inconsistent with a company's privacy promises constitute an unauthorized disclosure. These recent Commission orders also make clear that the use of "dark patterns," which have the effect of manipulating or deceiving consumers, including through use of user interfaces designed with the substantial effect of subverting or impairing user autonomy and decision-making, undercut an entity's assertion that consumers exercised "meaningful choice."

In response to public comments seeking more guidance on what constitutes an unauthorized disclosure under the Rule,[178] the Commission offers the following, non-exhaustive examples relating to authorization:

- **Example 1—Unauthorized Disclosure (Affirmative Misrepresentation):** A medication app offers a personal health record (not covered by HIPAA) which allows users to track information about their prescription medication history, such as prescription names, dosages, pharmacy and refill information, and the user's health conditions. The app voluntarily discloses PHR identifiable health information to third party companies for advertising and advertising-related analytics, in violation of the app's privacy representations to its users. The third parties that receive the PHR identifiable

[177] The 2009 Rule Commentary states: "[g]iven the highly personal nature of health information, the Commission believes that consumers would want to know if such information was read or shared without authorization." It further states that data sharing to enhance consumers' experience with a PHR is authorized only "as long as such use is consistent with the entity's disclosures and individuals' reasonable expectations" and that "[b]eyond such uses, the Commission expects that vendors of personal health records and PHR related entities would limit the sharing of consumers' information, unless the consumers exercise meaningful choice in consenting to such sharing. Buried disclosures in lengthy privacy policies do not satisfy the standard of 'meaningful choice.'" 74 FR 42967.
[178] TechNet at 4; Tranquil Data at 4.

health information are able to use the information for their own business purposes, such as to improve the third party's own products and services, to infer information about consumers, or to compile profiles about consumers to use for targeted advertising. These disclosures are not authorized under the Rule because they are inconsistent with consumer expectations—the disclosures violate the app's privacy representations, and consumers would also not expect that their PHR identifiable health information (which they input into the app to track their medications and health conditions) would be disclosed to, and used by, third party companies that use the data for their own economic benefit.

- By contrast, disclosures of PHR identifiable health information by the app in Example 1 would be authorized if made to service providers in the following circumstances: (1) the service providers assist with functions that are necessary to the operation and functioning of the medication app, or with services the consumer requested; (2) the service providers are contractually prohibited from using, sharing, or disclosing the PHR identifiable health information for any purpose beyond providing services to the medication app; and (3) the medication app's privacy notice clearly and conspicuously discloses the specific purposes for which it shares users' PHR identifiable health information with these service providers. Such authorized disclosures could include those to cloud storage providers that host user data in the health record in a secure fashion; payment processors who process user payments to the app; vendors that facilitate refill reminders or other communications from the app developer that directly relate to the provision of the personal health record or services the consumer requested; analytics providers that assist

with tracking analytics relating to the app's functionality[179]; or companies that help to detect, prevent, or mitigate fraud or security vulnerabilities. Such disclosures are authorized because they are consistent with consumer expectations. Importantly, this sharing is disclosed to consumers in a clear and conspicuous manner, and is essential, and limited to, sharing the PHR identifiable health information with service providers solely to provide users with a safe and reliable personal health record experience.

- **Example 2—Unauthorized Disclosure (Deceptive Omission).** The medication app from Example 1 shares PHR identifiable health information with a third party for purposes of targeting consumers with ads. The app does not disclose the sharing and also fails to obtain affirmative express consent from users whose information it shares. The third party company can use the PHR identifiable health information to market and advertise—on behalf of the medication app, on behalf of other companies, or on behalf of itself. It can also use the information to improve its own products and services. Such disclosures are not authorized because they are not consistent with consumer expectations (i.e., without disclosure and without affirmative express consent, consumers would not expect that their PHR identifiable health information would be shared, sold, or otherwise exploited for a purpose other than providing the user with a personal health record, and are neither essential nor limited to sharing the PHR identifiable health information solely to provide users with a safe and reliable personal health record experience). This conclusion is also consistent with Commission enforcement actions relating to the

[179] This would include an analytics provider whose services are essential to the proper functioning of the app and not tied to marketing or advertising—this includes analytics tools to assist with crash reporting or to assess usage patterns (such as the frequency of use of certain features).

sharing of health information (e.g., GoodRx and Easy Healthcare), and those relating to the sharing of other types of sensitive information.[180]

- **Example 3—Authorized Disclosure (Public Health Reporting):** A COVID-19 contact tracing app not covered by HIPAA allows users to self-report their COVID-19 diagnosis, and to notify the user's contacts of their diagnosis, or others with whom the individual may have come into physical contact. PHR identifiable health information about the individual's COVID-19 diagnosis is transmitted to public health authorities for public health-related purposes, such as public health reporting and analysis or to track areas where the virus is spreading the most rapidly. The contact tracing app discloses to users clearly and conspicuously the specific purposes for which it shares their PHR identifiable health information with public health authorities. These disclosures are authorized, and consistent with consumer expectations, because they are consistent with the company's relationship with the consumer (a PHR that allows a user to report their COVID-19 diagnosis in order to notify others) and are also appropriately disclosed.

Examples 1 and 3 provide guidance about scenarios in which limited disclosures of PHR identifiable health information are permitted without opt-in consent because it is necessary to provide a personal health record to a consumer, is consistent with consumer expectations, the sharing is disclosed to consumers, and (in the case of Example 1) the sharing is subject to protections like service provider agreements that limit the use of the data only for the purpose of providing that service to the consumer. Examples 1 and 3 are also consistent with HIPAA and

[180] *Fed. Trade Comm'n et. al. v. Vizio, Inc. et. al.*, No. 17-cv-00758 (D.N.J. 2017), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3024-vizio-inc-vizio-inscape-services-llc.

state health privacy laws.[181] For instance, HIPAA permits disclosures for treatment, payment, and operations without patient authorization.

The Commission notes that "breach of security" could cover more than just an unauthorized disclosure to a third party. For example, depending on the facts and scope of the authorizations, such as in the company's promises and disclosures to consumers, a "breach of security" could include unauthorized *uses*. There may be a "breach of security" where an entity exceeds authorized access to use PHR identifiable health information, such as where it obtains the data for one legitimate purpose, but later uses that data for a secondary purpose that was not originally authorized by the individual.

Finally, the Commission notes that unauthorized access or use of derived PHR identifiable health information may also constitute a breach of security. The Commission noted in its 2023 NPRM that PHR identifiable health information includes "health information derived from consumers' interactions with apps and other online services (such as health information generated from tracking technologies employed on websites or mobile applications or from customized records of website or mobile application interactions), as well as emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases)."[182]

4. Clarification of What Constitutes a "PHR Related Entity"

a. The Commission's Proposal Regarding "PHR Related Entity"

The NPRM proposed to revise the definition of "PHR related entity" in two ways. Consistent with its clarification that the Rule applies to health apps, the Commission proposed

[181] For example, Washington State's My Health, My Data Act permits sharing consumer health data to the "extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business." *See* RCW 19.373.030 (1)(b)(ii).
[182] 88 FR 37823.

amending the definition of "PHR related entity" to make clear that the Rule covers entities that offer products and services through the online services, including mobile applications, of vendors of personal health records. In addition, the Commission proposed revising the definition of "PHR related entity" to provide that entities that access or send unsecured PHR identifiable health information to a personal health record—rather than entities that access or send *any* information to a personal health record—are PHR related entities.

The Commission explained that the first change (to cover online services) was necessary as websites are no longer the only means through which consumers access health information online. The Commission explained that the second change – narrowing the scope of "PHR related entities" to entities that access or send *unsecured PHR identifiable health* information – was intended to eliminate potential confusion about the Rule's breadth and promote compliance by narrowing the scope of entities that qualify as PHR related entities.[183] The Commission identified remote blood pressure cuffs, connected blood glucose monitors, and fitness trackers as examples of internet-connected devices that could qualify as a PHR related entity when individuals sync them with a personal health record (e.g., a health app).[184] The Commission

[183] The proposed definition stated that a PHR related entity is an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that (1) offers products or services through the website, including any online service, of a vendor of personal health records; (2) offers products or services through the websites, including any online services, of HIPAA-covered entities that offer individuals personal health records; or (3) accesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record. Although the Rule is only triggered when there is a breach of security involving unsecured PHR identifiable health information, the Commission explained that it believed there is a benefit to revising the third prong of PHR related entity to make clear that only entities that access or send unsecured PHR identifiable health information to a personal health record – rather than entities that access or send any information to a personal health record – are PHR related entities. Otherwise, many entities could be a PHR related entity under the definition's third prong and such entities would then, in the event of a breach, need to analyze whether they experienced a reportable breach under the Rule. If an entity, per the proposed revision, does not qualify as a PHR related entity in the first place, there would be no need to consider whether it experienced a reportable breach. 88 FR 37825 n.54.

[184] The Commission explained that, for example, the maker of a wearable fitness tracker may be both a vendor of personal health records (to the extent that its tracker interfaces with its own app, which also accepts consumer inputs) *and* a PHR related entity (to the extent that it sends information to another company's health app). The

explained, however, that a grocery delivery service that sends information about food purchases to a diet and fitness app would not be a PHR related entity if it does not access unsecured PHR identifiable health information in a personal health record or send unsecured PHR identifiable health information to a personal health record.

The proposed Rule also revised § 318.3(b) by adding language establishing that a third party service provider is not rendered a PHR related entity when it accesses unsecured PHR identifiable health information in the course of providing services. The Commission explained that it did not intend for any entity (such as a firm performing attribution and analytics services for a health app) to be considered both a PHR related entity (to the extent it accesses unsecured PHR identifiable health information in a personal health record) and a third party service provider, which could create competing notice obligations and confuse consumers with notice from an unfamiliar company. The Commission explained that it considers such firms to be third party service providers that must notify the health app developers for whom they provide services, who in turn would notify affected individuals.

The Commission explained that distinguishing between third party service providers and PHR related entities would create incentives for responsible data stewardship and for de-identification because a firm would only become an entity covered by the Rule in relation to unsecured PHR identifiable health information. To the extent that firms must deal with unsecured PHR identifiable health information, PHR vendors would have incentives to select and retain service providers capable of treating data responsibly (e.g., by not engaging in any onward disclosures of data that could result in a reportable breach) and incentives to oversee

Commission noted that regardless of whether the maker of the fitness tracker is a vendor of personal health records or a PHR related entity, its notice obligations are the same: it must notify individuals, the FTC, and in some case, the media, of a breach. 16 CFR 318.3(a), 318.5(b). 88 FR 37825 n.55.

their service providers to ensure ongoing responsible data stewardship (which would avoid a breach).

The Commission observed that in most cases, third party service providers are likely to be non-consumer facing. The Commission noted that examples of PHR related entities would include, as noted above, makers of fitness trackers and health monitors when consumers sync their devices with a mobile health app. The Commission noted further that examples of third party service providers would include entities that provide support or administrative functions to vendors of personal health records and PHR related entities.

b. Public Comments Received Regarding "PHR Related Entity"

The Commission received numerous public comments about the changes to the definition of PHR related entity. Most commenters supported the Commission's approach.[185] One commenter, an industry association for advertisers, noted that addition of the term "unsecured" in the definition of "PHR related entity" created a limitation on the definition's scope that counterbalances the breadth of including "any online service" in the definition.[186] Moreover, this commenter noted, the addition of "unsecured" creates appropriate incentives for firms to secure PHR identifiable health information and to choose partners who will be good data stewards.[187] This commenter noted that limiting the definition to "unsecured" PHR identifiable health information was consistent with the original intent of the Rule, to cover only the most sensitive types of data not covered by HIPAA.[188]

A few commenters proposed changes to the definition of "third party service provider"

[185] ANI at 1; AAFP at 3; AHIMA at 3; AHIOS at 4; AOA at 3; CARIN Alliance at 3; CDT at 12; CHIME at 3; Confidentiality Coal. at 6; Consumer Rep.'s at 6; CHI at 5; DirectTrust at 4; EFF at 2; EPIC at 7.
[186] NAI at 4-5.
[187] *Id.* at 5.
[188] *Id.* at 4.

to further distinguish the term from "PHR related entity." One commenter recommended defining "third party service provider" as an entity that only processes data.[189] This commenter argued that the Commission could then impose liability on service providers for further use, sale, disclosure for incompatible purposes.[190] Another commenter recommended aligning the definition of "third party service provider" with the definition of "business associate" under HIPAA.[191]

Some commenters raised concerns that the Commission's approach did not provide sufficient clarity for companies trying to understand their obligations as either a third party service provider or PHR related entity.[192] Some commenters requested more examples of types of firms falling within each definition (e.g., examples clearly establishing the status of health data brokers, health marketing firms, search engines, email providers, cloud storage providers)[193]— to facilitate compliance,[194] avoid overlapping notice requirements[195] and to prevent a loophole through which firms may attempt to avoid obtaining consumers' authorization for data disclosures and to avoid providing breach notifications.[196] One commenter urged the Commission to exempt from the definition of "PHR related entity" any firm that complies with the privacy and data security requirements of HIPAA.[197]

In response to the Commission's request for comment on whether an analytics firm would be a third party service provider, many commenters responded that an analytics firm

[189] FPF at 10.
[190] *Id.*
[191] AdvaMed at 8.
[192] SIIA at 3; CARIN Alliance at 4.
[193] AHIMA at 3-4; AMIA at 3-4; CHI at 5; Direct Trust at 1; Light Collective at 4-5.
[194] SCRS at 1.
[195] NAI at 5.
[196] MRO at 3.
[197] AdvaMed at 5.

should fall within that definition[198] for the reasons the Commission articulated: It would be confusing to consumers to receive a notice from a back-end service provider rather than the firm with whom the consumer has the relationship, and categorizing analytics firms (and firms that provide other services) as service providers will create incentives for PHR vendors and PHR related entities to choose their service providers with care. A few commenters, however, expressed concern about covering advertising, analytics, and cloud firms — and health information service providers ("HISPs") more generally — as they are unable to determine whether the data they receive contains unsecured PHR identifiable health information; only the vendor of the PHR knows what their data transmissions contain.[199] One commenter urged the Commission to address the data recipient's unawareness of the content of the data by creating a safe harbor that exempts advertising, analytics and cloud providers that contractually limit their customers, vendors, or partners from sharing health information with them.[200]

c. The Commission Adopts the Proposed Changes to "PHR Related Entity"

After considering the comments received, the Commission adopts the proposed changes regarding "PHR related entity" without further change. The Commission affirms that (1) PHR related entities include entities offering products and services not only through the websites of vendors of personal health records, but also through any online service, including mobile applications; (2) PHR related entities encompass only entities that access or send unsecured PHR identifiable health information to a personal health record; and (3) while some third party service providers may access unsecured PHR identifiable health information in the course of providing services, this does not render the third party service provider a PHR related entity.

[198] NAI at 5; TMA at 3; Consumer Rep.'s at 11.
[199] CCIA at 7-8; CTA at 9-10; SIIA at 3; Direct Trust at 5.
[200] CTA at 13.

In response to commenters who expressed concern that certain data recipients will not be able to understand their obligations under the Rule because they are unaware of the content of the data transmissions they receive, the Commission highlights § 318.3(b), which states: "For purposes of ensuring implementation of this requirement, vendors of personal health records and PHR related entities shall notify third party service providers of their status as vendors of personal health records or PHR related entities subject to this Part." This requirement puts data recipients on notice about the potential content of the data transmissions they receive.

Firms may also facilitate compliance by stipulating by contract whether transmissions of data will contain unsecured PHR identifiable health information. Both the sender and recipient of the data can monitor for compliance with those contractual agreements through the use of automated tools, internal auditing, external auditing, or other mechanisms, as appropriate to the size and sophistication of the firms and the sensitivity of the data. For example, a large advertising platform that has routinely received unsecured PHR identifiable health information, notwithstanding partners' promises not to send this information, may have different obligations to monitor the data it receives than small firms that do not engage in high-risk activities where the contract precludes sending such data and there is no history of such transmissions.

The Commission believes that this approach – notice to service providers pursuant to § 318.3(b) coupled with contracts and oversight – is more appropriate than creating a safe harbor in the Rule that exempts firms that enter into contracts, as there is evidence from FTC cases that firms do not always abide by contractual obligations to safeguard data.[201]

[201] Compl. at ¶ 21, *In the Matter of Flo Health, Inc.,* FTC File No. 1923133 (Jan. 13, 2021), *https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc*; Compl. at ¶ 14(d), *In the Matter of UPromise, Inc.*, FTC File No. 1023116 (Mar. 27, 2012), *https://www.ftc.gov/legal-library/browse/cases-proceedings/102-3116-c-4351-upromise-inc*; *Cf.* Compl. at ¶ 40, *U.S. v. Easy Healthcare Corporation*, No. 1:23-cv-3107 (N.D. Ill. 2023), *https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-*

The Commission declines to change the definition of "third party service provider" to distinguish it further from a "PHR related entity," for two reasons. First, the Commission notes that the current definitions of "third party service provider" and "PHR related entity" align closely with the language prescribed by section 13407 and section 13424(b)(1)(A) of the Recovery Act. Jettisoning the current language entirely, as some commenters suggested, would not be consistent with the Recovery Act's requirements. Second, the Commission believes that the current language, in conjunction with the examples provided below, will provide sufficient guidance to the market as to which types of firms fit within each definition.

In response to comments that requested examples of the types of firms that fall into the category of "third party service provider" or "PHR related entity," the Commission provides the following examples. The Commission believes that these examples, in conjunction with the language in § 318.3(b), will provide sufficient clarity about the obligations of third party service providers and PHR related entities to promote compliance, avoid overlapping notice, and prevent loopholes.

- **Example 1:** Four separate firms provide data security, cloud computing, advertising and analytics services to a health app (a personal health record), as specified by their service provider contracts, for the health app vendor's benefit. To perform the services specified in their respective contracts, the firms access unsecured PHR identifiable health information. The firms are "third party service providers" of the vendor of the personal health record (the maker of the health app) because they provide services to a vendor of a personal health record (the maker of the health app) in connection with the offering or

corporation-us-v (alleging that the defendant's disclosures of consumers' health information violated the policies of platforms to which it had agreed).

maintenance of the app, and they access unsecured PHR identifiable health information as a result of these services. In the event of a breach, they should abide by their obligations as third party service providers.

- **Example 2:** An analytics firm provides analytics services to a health app (a personal health record). The analytics firm and health app vendor do not have a customized service provider contract, although the health app vendor agrees to the analytics firm's standard terms of service. The analytics firm accesses unsecured PHR identifiable health information (device identifier and whether the consumer has paid for therapy). The analytics firm uses that data both to provide analytics services to the health app and for its own benefit, for research and development and product improvement. The analytics firm is a third party service provider to the extent that it provides analytics services to the health app for the health app's benefit because it is then providing services to a vendor of a PHR in connection with the offering of the PHR and accessing unsecured PHR identifiable health information as a result of such services. However, the analytics firm is a PHR related entity, rather than a third party service provider, to the extent that it offers its services through the health app for its own purposes (i.e., for research and development and product improvement) rather than to provide the services. In the event of a breach, the analytics firm must fulfill its notification obligations under the Rule according to which function it was performing in connection with the breach. If the functions are indistinguishable, then, pursuant to § 318.3(b), the Commission will consider the firm a third party service provider for policy reasons: a firm that functions, at least in part, as a service provider may not be consumer-facing, such that the consumer may be surprised by a breach notification from that entity. As a policy matter, it is better

for the consumer to receive notice from the health app with whom the consumer directly interacts.

- **Example 3:** A health tracking website (a personal health record) integrates a search bar branded with its maker's logo, which enables its maker (a search engine firm) to offer its services through the website. The search engine firm is a PHR related entity because it offers its services through the website, which is a personal health record. The search bar branded with its maker's logo is consumer-facing, so the consumer would not be surprised to receive a notice from that company if it experiences a reportable breach. By contrast, if the health tracking website had contracted with the search engine firm to provide back-end search services to the website (rather than offering its own branded product or service through the website), and the search engine firm had accessed unsecured PHR identifiable health information as a result of such services, it would be a third party service provider. In the event of a breach, it should abide by its obligations as a third party service provider.
- **Example 4:** Digital readings from a fitness tracker offered by Company A can be integrated into a sleep app offered by Company B (in which the consumer may input other health information). Company A is a PHR related entity to the extent that it offers its fitness tracker product through an online service (Company B's sleep app), and to the extent that it sends unsecured PHR identifiable health information (fitness tracker readings) to a personal health record (the sleep app).

5. Facilitating Greater Opportunity for Electronic Notice

a. The Commission's Proposal Regarding Electronic Notice

The Commission proposed to authorize expanded use of email and other electronic means

of providing clear and effective notice of a breach to consumers. In furtherance of this objective, the Commission proposed to update § 318.5 to specify that vendors of personal health records or PHR related entities that discover a breach of security must provide written notice at the last known contact information of the individual. Such written notice may be sent by electronic mail, if an individual has specified electronic mail as the primary contact method, or by first-class mail. The Commission proposed defining "electronic mail" in § 318.2 to mean email in combination with one or more of the following: text message, within-application messaging, or electronic banner. The Commission further specified that any notification delivered via electronic mail should be clear and conspicuous, and the proposed Rule defined "clear and conspicuous." To assist entities that are required to provide notice to individuals under the Rule, the Commission developed a model notice for entities to use to notify individuals.[202]

b. Public Comments Received Regarding Electronic Notice

Nearly every comment submitted on this proposed change supported the Commission's efforts to update the Rule to allow for greater electronic notice.[203] One commenter noted that electronic notices increase the likelihood that individuals will receive the notice, may reduce the time it takes for individuals to receive notice, and reduce the burden on entities providing notice.[204] Many commenters also supported the Commission's efforts to provide notice via more than one channel through the new definition of "electronic mail."[205]

[202] This model notice was attached as Appendix A to the NPRM. 88 FR 37837.
[203] AHIP at 5; AAFP at 3; AHIMA at 5; AHIOS at 3; Anonymous 3 at 1; Anonymous 10 at 1; Beth Barnett; CARIN Alliance at 7; CHI at 5-6; CHIME at 4; Consumer Reports at 8-9; CTA at 21; EPIC at 10; HIMSS at 4; George Mathew at 1; MRO at 3; NAI at 7; Dharini Padmanabhan at 1; Nancy Piwowar at 1. One commenter also stated that while there are clear advantages to allowing increased use of electronic notification of data breaches, this notification method could also increase the likelihood that breaches escape public scrutiny. Identity Theft Res. Ctr. ("ITRC") at 2.
[204] AdvaMed at 5.
[205] AAFP at 3; AHIMA at 5; Anonymous 3 at 1; CARIN Alliance at 7; CHIME at 4; CCIA at 7; EPIC at 10; NAI at 7.

However, not all commenters agreed with the Commission's proposal and some commenters offered other suggestions. Some objected to defining "electronic mail" to mean anything more than "email," stating that electronic mail is commonly understood to mean email and nothing else.[206] A few commenters noted that defining multiple forms of electronic notice could result in entities collecting more information than necessary (and consumers having to provide more information than needed) in order to comply with the Rule.[207] Others preferred a single notice, arguing that multiple forms of notice is burdensome and could result in over-notification, confusion, and notice fatigue among consumers.[208] One commenter stated that the Commission should revise the definition of "electronic mail" to mean "one or more of the following that is reasonable and appropriate based on the relationship between the individual and the relevant vendor of personal health records or PHR related entity: email, text message, within-application messaging, or electronic banner."[209] Another commenter encouraged the FTC to clarify that the in-app messaging method must include push notifications in the event of a breach so consumers are made aware of a breach as soon as possible.[210] One commenter urged the Commission to specify in § 318.5(i) that a banner notice in the affected app or a website home page notice must be posted for a period of 90 days.[211] Another commenter noted that the different mechanisms listed in the proposed rule are not equivalent – this commenter noted that some are push notifications that a consumer is likely to see without directly interacting with the application, website, or device and some require consumer interaction with the application,

[206] ACLA at 5; Mass. Health Data Forum ("MHDF") at 9.
[207] Consumer Rep.'s at 7-8; CTA at 22. Consumer Reports further suggested that the Commission clarify that substitute notice may be effectuated under the Rule via text message, in-app messaging, or electronic banners for consumers that do not wish to share a mailing or email address. Consumer Rep.'s at 8.
[208] AdvaMed at 6; ACLA at 5; AHIP at 5; CTA at 21-22;
[209] AdvaMed at 6.
[210] AHIMA at 5.
[211] TechNet at 5.

website, or device in order to see the notification.[212] This commenter recommended that the requirement be selection of one push notification but that additional options like in-app notifications and website banners be supported as additional, secondary notice options.[213] One commenter stated that the FTC may want to consider adding a provision allowing an individual to request a copy of the notice in other accessible formats, such as for hearing- or vision-impaired people, or in a non-English language.[214] Another commenter argued that the Commission should take into consideration TCPA and CAN-SPAM compliance regarding the delivery of electronic notification. Another commenter stated that the Commission's proposal to require two contact methods imposes a higher requirement than HIPAA and state breach notification laws.[215]

Many commenters endorsed the Commission's proposal that any notification delivered via electronic mail should be "clear and conspicuous," a newly defined term in the Rule.[216] One commenter stated that consistent with FTC's desire for entities to provide a clear and conspicuous notice, the Commission should consider requiring an email subject line that starts with "Breach of Your Health Information" so that attention is appropriately drawn to the importance of the message content.[217] One commenter disagreed with the new definition, arguing that the definition is unnecessary and confusing, and urged the Commission to insert the "clear and conspicuous" definition directly into § 318.5 of the Rule.[218]

Regarding the model notice, nearly all who commented on this topic urged the

[212] MHDF at 10.
[213] *Id.*
[214] AHIP at 5.
[215] CHI at 6.
[216] AMA at 5; CHIME at 5; EPIC at 9.
[217] TMA at 4.
[218] NAI at 7.

Commission to make the model notice voluntary.[219] One commenter suggested that using the model should be a safe harbor that shields entities from enforcement.[220]

c. The Commission Adopts Changes Regarding Electronic Notice

The Commission adopts without change the modifications regarding § 318.5 involving electronic notice and adopts without change the definition of "electronic mail" in § 318.2. The Commission declines to make the other changes commenters requested. First, the Commission believes it is critical, especially given how consumers are accessing information today, to modernize the methods of notice to facilitate greater opportunities for electronic notice. The Commission believes the changes to § 318.5 and the new definition of "electronic mail"[221] in § 318.2 accomplish this objective.

In response to concerns raised about the two-part electronic notice, the Commission agrees with commenters who stated it increases the likelihood that individuals will encounter such notices.[222] The Commission does not agree that it is burdensome for entities to comply

[219] AdvaMed at 6; AHIP at 6; AMA at 6; CCIA at 7; CHI at 6; Consumer Rep.'s at 8-9; NAI at 7-8. One commenter stated that making the model notice mandatory can lead to industry consistency and it may be easier for consumers to understand the message and the contents if they are familiar with a uniform, standardized notice. AHIMA at 5. While the Commission generally agrees that uniform, consistent notices assist with consumer comprehension, the Commission declines to make the model notice compulsory because the facts and circumstances of each breach will vary. Plus, § 318.6 sets forth certain required elements of the content of the notice, so the presence of these elements in all breach notices achieves some degree of consistency across notices.

[220] AHIP at 6.

[221] The Commission disagrees with the commenters who urged the Commission to avoid defining "electronic mail" to mean anything more than "email." ACLA at 5; MHDF at 9. The definition in § 318.2 is clear and unambiguous. Plus, section 13402(e)(1) of the Recovery Act requires that notification be provided via "written notification by first-class mail" or "electronic mail." Accordingly, the Commission must use "electronic mail."

[222] AAFP at 3-4 (noting that AAFP appreciates "the proposed structure of providing notice in two different electronic formats to increase the likelihood individuals will see them"); CHIME at 5 ("CHIME is supportive of the FTC's approach to revise the "method of notice section" and to structure the breach notification in two parts in order to increase the likelihood that consumers encounter the notice."); EPIC at 10 ("By requiring email *and* an in-app or website notice option, the expanded definition enables entities to have the best chance at notifying consumers regardless of whether they reliably check their email or continue to use the entity's app or website."). The Commission also disagrees with the commenter who recommended that the Commission abandon the two-part notice and create a new definition of "electronic mail" where, for example, only a website notice alone would satisfy the notice requirement if such a notice was "reasonable and appropriate." AdvaMed at 6. The Commission disagrees with this approach and declines to adopt it.

with this requirement. For example, an entity who complies with the notice requirement by notifying consumers via email plus posting a website notice likely would not need to expend significant additional time and resources by issuing the second part of the notice (i.e., the website notice), and any "cost" of posting such a notice is outweighed by the benefit to consumers of learning of a breach involving their health information. The Commission also is not persuaded that consumers who, for example, receive an email about a breach coupled with an in-app notice about the same breach will be confused. The Commission believes consumers will understand that such notices relate to the same incident, especially given the Rule's requirement that the notices be "clear and conspicuous." The Commission also does not find it problematic that the Rule requires notice effectuated via "electronic mail" to occur via two methods while other breach notice laws require one method. The Commission also notes that while these amendments are intended to facilitate greater electronic notice, the Rule still permits notice via first-class mail. Accordingly, the contention that this Rule requires two methods of electronic notice is incorrect.

The Commission also declines, in response to public comments,[223] to mandate how notifications are effectuated when sent via "electronic mail," as the Commission believes it is important to not be overly prescriptive given rapidly changing technologies. The Commission emphasizes though, as described below, that the notice must satisfy the Rule's definition of "clear and conspicuous."

Nor does the Commission believe, as some commenters argued, that the two-part electronic notification will result in additional collections of information by notifying entities.

[223] *See supra* notes 210-213.

The Commission agrees with commenters who stated that entities are generally already collecting the information needed for notice via "electronic mail" and a data minimization issue does not exist.[224]

In response to the commenter who suggested that the FTC consider adding a provision allowing an individual to request a copy of the notice in other accessible formats, such as for hearing- or vision-impaired people, or in non-English languages,[225] the Commission previously addressed a similar comment in the 2009 Rule Commentary. There, the Commission noted that Section 13402(e)(l) of the Recovery Act requires that notification be provided via "written notification by first-class mail" or "electronic mail." The Commission emphasized then, as we do today, that the Rule does not preclude notifications in accessible formats. The Commission supports their use in appropriate circumstances, in addition to the forms of notice prescribed by the Rule.[226]

The Commission also adopts without modification the definition of "clear and conspicuous." The Commission agrees with the commenter who indicated that it is imperative that a breach notice be reasonably understandable and call attention to the significance of the information that is included in the notice.[227] The Commission believes that its definition of "clear and conspicuous" will assist in achieving this objective. The Commission declines, however, to mandate specific language for the email subject line to satisfy the Rule's "clear and conspicuous" requirement, as one commenter had suggested.[228] The Commission emphasizes, however, that the clear and conspicuous requirement would require a notifying entity to use an

[224] CARIN Alliance at 6; EPIC at 10.
[225] *See supra* note 214.
[226] 74 FR 42972.
[227] AMA at 5.
[228] *See supra* note 217.

email subject line that draws the reader's attention to the email notice. The Commission also declines to adopt the suggestion that the definition of "clear and conspicuous" be incorporated directly into § 318.5. The Commission believes the entities seeking information on what "clear and conspicuous" means will find it clearer to consult the definition in § 318.2.

Turning to the model notice,[229] as the Commission noted in the NPRM, the model was intended for entities to use, in their discretion, to notify individuals, and the Commission adopts the same position here.[230] The model is voluntary and while the Commission believes it represents a best practice, using the model is not required to achieve compliance with the Rule.

The Commission declines to adopt the position that use of the model notice provides a safe harbor, although the Commission would take into consideration in an enforcement action an entity who follows the model notice. Further, the Commission notes that an entity who follows the model notice can nevertheless violate the Rule in other ways. For example, an entity could follow the model notice but fail to provide timely notice. In such instances, providing a safe harbor because the entity utilized the model notice would be inappropriate.

6. Revisions to the Required Content of Notice

a. The Commission's Proposal Regarding Content of Notice

The Commission proposed five changes to the content of the notice. First, in § 318.6(a), as part of relaying what happened regarding the breach, the Commission proposed that the notice to individuals also include a brief description of the potential harm that may result from the breach, such as medical or other identity theft. Second, the Commission proposed to amend the requirements for the notice under § 318.6(a) to include the full name, website, and contact

[229] The model notice is found in Appendix A.
[230] 88 FR 37827.

information (such as a public email address or phone number) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security, if this information is known to the vendor of personal health records or PHR related entity (such as where the breach resulted from disclosures of users' sensitive health information without authorization). Third, the Commission proposed modifications to § 318.6(b), which requires that the notice include a description of the types of unsecured PHR identifiable health information that were involved in the breach. The Commission proposed that this exemplar list be expanded to include additional types of PHR identifiable health information, such as health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, and device identifier. Fourth, the Commission proposed revising § 318.6(d) of the Rule to require that the notice to individuals include additional information providing a brief description of what the entity that experienced the breach is doing to protect affected individuals, such as offering credit monitoring or other services. Fifth, the Commission proposed modifying § 318.6(e) so that the contact procedures specified by the notifying entity must include two or more of the following: toll-free telephone number; email address; website; within-application; or postal address.

b. Public Comments Received Regarding Content of Notice

1. Proposal that Notice Include Description of Potential Harm that May Result from a Breach

The Commission's proposal to modify § 318.6(a) to include in the notice to individuals a brief description of the potential harm that may result from a breach drew a wide range of

comments. On the one hand, many commenters supported the Commission's proposal.[231] For example, one commenter noted that this proposal would help individuals better understand the connection between the information breached and the potential harm that could result from the breach of such information.[232] Other commenters stated that providing the potential harms from a breach better equips consumers to address injuries and mitigate harms from it.[233] One commenter stated that including some potential harms would be helpful, but notifying entities should also include language in the notice stating that other harms may occur.[234] This same commenter suggested that the Commission consider selecting the most common types of breaches and listing some but not all of the potential consequences from each.[235]

On the other hand, many commenters criticized this proposal.[236] Some commenters argued that this proposal will result in notifying entities having to speculate about potential harms that may never occur or providing a list of harms that may be incomplete.[237] Others pointed out that notifying individuals about potential harms could cause consumer anxiety, consumer confusion, and detract from actions the individuals should take.[238] One commenter noted that the Commission's proposal might lead consumers to believe the harms listed in the notice are the only possible harms from a breach, when in fact consumers may suffer other harms not disclosed in the notice.[239] This same commenter also noted that it is opposed to entities

[231] AAFP at 4; AMA at 6; AOA at 5; Anonymous 3; AHIOS at 3; CARIN Alliance at 7-8; CHIME at 3, 6; Consumer Reports at 9-10; EFF at 2; EPIC at 10-11; HIMSS at 3-4; ITRC at 2; Members of the House of Representatives at 1-2; Dharini Padmanabhan at 1.
[232] AMA at 6.
[233] Consumer Rep.'s at 9-10; EPIC at 10-11.
[234] MHDF at 10-11.
[235] *Id.*
[236] AdvaMed at 6-7; AHIP at 6; ACLA at 4-5; Confidentiality Coal. at 7; CTA at 23-24; MHDF at 10; NAI at 9.
[237] AdvaMed at 6-7; AHIP at 6; MHDF at 10; NAI at 9.
[238] ACLA at 4-5; AMIA at 5; NAI at 9.
[239] MHDF at 10.

stating there are no known harms that may result from a breach solely because a notifying entity is unaware of any specific bad outcomes.[240]

2. Proposal that Notice Include Full Name, Website and Contact Information of Third Parties that Acquired Unsecured PHR Identifiable Health Information

Next, the Commission proposed to amend the requirements for the notice under § 318.6(a) to include the full name, website, and contact information (such as a public email address or phone number) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security. Although several commenters supported this proposal,[241] many others pointed out that it is problematic in certain circumstances.[242] A few commenters noted that the proposal is ill-suited for security breaches, such as a hacking, where providing consumers with the name and contact information of an actor who committed a security breach (e.g., a hacker) could result in further malicious action against the target entity.[243] One commenter noted that for security breaches, the malicious actor or hacker would not be responsive to consumers.[244] Further, one commenter noted that this requirement could hamper law enforcement efforts.[245] One commenter also indicated that this requirement could frustrate investigative efforts or have a chilling effect on an inadvertent recipient from reporting a wrongful disclosure.[246]

---

[240] *Id.* at 10-11.
[241] AAFP at 4; AHIMA at 5-6; AMA at 6; AMIA at 5; AOA at 5; CARIN Alliance at 7; Consumer Rep.'s at 9-10; EFF at 2; EPIC at 10-11; HIMSS at 3-4; ITRC at 2; Members of the House of Representatives at 1-2.
[242] ACLA at 4-5; AHIP at 6; CHI at 6; Confidentiality Coalition at 7; CTA at 24.
[243] ACLA at 4-5; Confidentiality Coal. at 7.
[244] Confidentiality Coal. at 7.
[245] CTA at 24.
[246] AHIP at 6.

3. Proposal that Notice Include Description of Types of Unsecured PHR Identifiable Health Information Involved in a Breach

Third, the Commission proposed modifications to § 318.6(b), which requires that the notice to individuals include a description of the types of unsecured PHR identifiable health information that were involved in the breach. The Commission proposed that this exemplar list be expanded to include additional types of PHR identifiable health information, such as health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, and device identifier. Several commenters supported this proposal.[247] One commenter noted that it is important for consumers to receive notice of the specific types of PHR identifiable health information involved in a breach, given that the exposure of health information can lead to a wide spectrum of harms.[248] Another commenter stated that providing individuals with a more expansive list of exposed data points will also give them a more complete picture of the risks they face.[249]

4. Proposal that Notice Include Description of What Entity is Doing to Protect Affected Individuals

Fourth, the Commission proposed revising § 318.6(d) of the Rule to require that the notice to individuals include additional information providing a brief description of what the entity that experienced the breach is doing to protect affected individuals, such as offering credit monitoring or other services. This proposal attracted support from multiple commenters.[250] One commenter stated that informing individuals about these steps is important so that they know

[247] AAFP at 4; AHIMA at 6; AMA at 6; AOA at 5; CARIN Alliance at 7; Consumer Rep.'s at 9-10; Ella Balasa at 2; HIMSS at 3-4; ITRC at 2; NAI at 9.
[248] Light Collective at 2.
[249] ITRC at 2.
[250] AAFP at 4; AMA at 6; AOA at 4; CARIN Alliance at 7-8; HIMSS at 3-4; ITRC at 2.

what additional actions they should take to protect themselves from potential harm.[251] Another similarly stated that knowing what the notifying entity is doing to protect affected individuals can help consumers who are considering making purchase decisions for fraud detection or credit monitoring.[252] One commenter stated that requiring notifying entities to share this information will incentivize them to take proactive measures to mitigate harms to consumers.[253]

Some commenters, however, raised concerns about this proposal. For instance, one commenter believed that the Rule already encompasses this requirement and therefore the Commission's proposal could result in duplicative information being provided in the notice.[254] Another commenter stated that the FTC needs to go further in ensuring that notification requirements help consumers understand what remedies are available when their health information is breached.[255]

5. Proposal that Notice Include Two or More Contact Procedures

Fifth, the Commission proposed amendments to § 318.6(e) so that the contact procedures specified by the notifying entity in its breach notification must include two or more of the following: toll-free telephone number; email address; website; within-application; or postal address. Many commenters expressed support for this proposal.[256] One commenter noted that multiple contact options ensures that victims of all backgrounds and technical capabilities are able to contact the notifying entity to learn more about how to protect themselves after a

[251] AMA at 6.
[252] AHIMA at 5-6.
[253] Consumer Rep.'s at 9-10.
[254] Confidentiality Coal. at 7.
[255] Light Collective at 6-7.
[256] AAFP at 4; AHIMA at 6; AHIP at 5; Anonymous 3 at 1; AOA at 5; CARIN Alliance at 8; Consumer Rep.'s at 9-10; EPIC at 9-10; HIMSS at 3-4; ITRC at 2; Dharini Padmanabhan at 1.

breach.[257] Another commenter noted that providing multiple contact options encourages and facilitates communication between the individual and the notifying entity.[258] One commenter, however, expressed concern that the proposal is burdensome, the HIPAA breach notice rule requires only one method of contact, and HHS has not identified any concerns with individuals having difficulty obtaining information from covered entities using one contact method under HIPAA's breach notice rule.[259]

c. Commission Changes Regarding Content of Notice

1. Commission Declines to Adopt Proposal that Notice Include Description of Potential Harm that May Result from a Breach

The Commission believes, in light of the public comments, that the downsides of requiring in the notice a description of the potential harms that may result from a breach outweigh the upsides. The Commission is concerned about requiring a consumer notice to include possible harms that may never materialize. In such cases, consumers may experience needless anxiety and take actions that are not necessary, leading to consumer frustration. The Commission also is concerned that this proposal may result in entities describing potential harms so generically that the description provides minimal value to consumers, or, alternatively, that entities will provide a laundry list of potential harms, making such a list meaningless to consumers. The Commission also agrees with one commenter who noted that this proposal might lead consumers to believe the harms listed in the notice are the only possible harms from a breach, when in fact consumers may suffer other harms not disclosed in the notice.[260]

[257] AHIMA at 6.
[258] AMA at 6.
[259] AdvaMed at 6-7.
[260] MHDF at 10.

Accordingly, the Commission declines to adopt this proposal.[261] The Commission believes that the remaining elements of the content of the notice will supply individuals with sufficient information about a breach, especially given the other modifications to § 318.6. The Commission also emphasizes that in certain cases where harms are concrete and known, notifying entities should as a best practice inform individuals about those harms in the notice.

2. The Commission Modifies Proposal that Notice Include Full Name, Website, and Contact Information of Third Parties that Acquired Unsecured PHR Identifiable Health Information

In light of the public comments, the Commission is modifying § 318.6(a) to require notifying entities to provide the full name or identity (or where providing name or identity would pose a risk to individuals or the entity providing notice, a description) of the third parties that acquired the PHR identifiable health information as a result of a breach of security.[262] The Commission believes it is important for consumers to know who acquired their PHR identifiable health information as a result of a breach. At the same time, the Commission acknowledges that in some scenarios it could be problematic to require notifying entities to provide the contact information of those who acquired PHR identifiable health information.

Accordingly, this revised provision is intended to still provide individuals with information about who acquired their health information. Under § 318.6(a), notifying entities are required to provide the full name or identity of the third parties that acquired the PHR identifiable health information as a result of a breach of security, except where providing the full name or identity of the third parties would pose a risk to affected individuals or the entity

[261] The Commission has updated the model notice in Appendix A to reflect this change.
[262] The Commission has updated the model notice in Appendix A to reflect this change.

providing notice. In cases where providing the name or identity of the third parties that acquired the PHR identifiable health information as a result of a breach of security would pose a risk to affected individuals or the entity providing notice (e.g., providing the name of hacker could subject affected individuals or the entity providing notice to further harm), § 318.6(a) permits notifying entities to describe the type of third party (e.g., hacker) who acquired individuals' PHR identifiable health information.

3. The Commission Adopts Proposal that Notice Include Description of Types of Unsecured PHR Identifiable Health Information Involved in a Breach

The Commission agrees with the many public comments supporting this proposal.[263] The Commission concurs with the commenter who noted it is important for consumers to receive notice of the specific types of PHR identifiable health information involved in a breach,[264] and the commenter who stated that providing affected individuals with a more expansive list of health data points implicated in a breach will help them better understand the risks they face.[265] The Commission adopts this proposal without modification.

4. The Commission Adopts Proposal that Notice Include Description of What Entity is Doing to Protect Affected Individuals

Several commenters supported the Commission proposal that the notice to individuals include a description of what the notifying entity is doing to protect affected individuals.[266] The Commission concurs with the commenter who stated that informing affected individuals about

[263] *See supra* note 247.
[264] *See supra* note 248.
[265] *See supra* note 249.
[266] *See supra* note 250.

the steps notifying entities are taking to protect them is important so that affected individuals know what additional actions they should take to protect themselves from potential harm.[267] The Commission similarly agrees with the commenter who stated that knowing what the notifying entity is doing to protect affected individuals can help consumers who are considering making purchase decisions like fraud detection or credit monitoring.[268] The Commission also agrees with the commenter who stated that requiring notifying entities to share information about what they are doing to protect affected individuals will incentivize notifying entities to take proactive measures to mitigate harms to consumers.[269]

In response to the one commenter who noted that the 2009 Rule already includes this proposed requirement,[270] the Commission notes that § 318.6(d) from the 2009 Rule requires notifying entities to include in the notice to individuals what the entity is doing to investigate the breach, to mitigate any losses, and to protect against any further breaches. Accordingly, under the 2009 Rule, there is no explicit requirement for the notifying entity to state in the individual notice what the entity is doing to protect affected individuals. Given this, the Commission does not believe individuals will receive duplicative information.

In response to the commenter who argued that the Commission needs to help consumers understand post-breach remedies,[271] the Commission believes that this concern is addressed by the combination of § 318.6(c), which requires notifying entities to include in the notice steps individuals should take to protect themselves from potential harm resulting from the breach, and

[267] *See supra* note 251.
[268] *See supra* note 252.
[269] *See supra* note 253.
[270] *See supra* note 254.
[271] *See supra* note 255.

§ 318.6(d), which requires notifying entities to include in the notice the steps the notifying entity is taking to protect affected individuals following the breach.

The Commission adopts proposed § 318.6(d) without modification.

5. The Commission Adopts Proposal that Notice Include Two or More Contact Procedures

In response to the comment that providing two or more contact procedures in the notice is burdensome,[272] the Commission believes that if this proposal results in any burden to notifying entities, such burden will be minimal given the ease with which compliance with this provision can be achieved, and outweighed by the benefits to consumers who will have increased options to communicate with notifying entities. Second, in response to the comment that the HIPAA Breach Notification Rule requires only one contact method,[273] the Commission notes that while there are many similarities between the FTC's and HHS' respective breach notification rules and the agencies have consulted to harmonize the two rules, there are differences between them, and the Commission believes it is important to update this provision to reflect new modes of communication and facilitate greater opportunities for communication between affected individuals and notifying entities.

The Commission notes that multiple commenters supported this proposal.[274] Specifically, the Commission agrees with the commenter who stated that multiple contact procedures enables greater opportunities for affected individuals to communicate with notifying entities.[275] The Commission also agrees with the commenter who noted that multiple contact

[272] *See supra* note 259.
[273] *Id.*
[274] *See supra* note 256.
[275] *See supra* note 258.

options ensures that affected individuals from all backgrounds and technical capabilities are able to contact the notifying entity following a breach.[276] The Commission therefore adopts proposed § 318.6(e) without modification.

7. Timing of Notice to the FTC

a. The Commission's Proposal Regarding Timing of Notice

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. Regarding the notification timeline to the FTC, the Commission sought comment on whether it should extend the timeline to give entities more time to investigate breaches and better ascertain the number of affected individuals or whether an extension would simply facilitate dilatory action and minimize the opportunity for an important dialogue with Commission staff during the fact-gathering stage immediately following a breach.

b. Public Comments Regarding Timing of Notice

Several commenters expressed support for extending the notification timeline to the FTC.[277] 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.[278] Others commented that the existing requirement diverts key resources from investigating potential breaches, indicating that when a

[276] *See supra* note 257.
[277] AdvaMed at 9; AHIP at 7; ACLA at 3-4; ATA Action at 2; CCIA at 8; CHI at 6; CTA at 20-21; TechNet at 5.
[278] AdvaMed at 9; ACLA at 3-4; AHIP at 7; TechNet at 5-6.

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.[279]

Several commenters urged the FTC to align the timeframe to notify the FTC with the timing requirement under HIPAA's Health Breach Notification Rule,[280] which requires notification to the Secretary of HHS without unreasonable delay and in no case later than 60 calendar days following a breach.[281] One commenter, irrespective of HIPAA, suggested that the Commission give entities up to 60 days to investigate a breach and provide notification to the Commission.[282] One commenter recommended that the FTC adopt a "risk-based" notification approach whereby the agency could create a shorter notification timeline for high-risk incidents and a longer notification timeline or even no notification for low-risk incidents.[283]

c. The Commission Adopts Changes to the Timing of Notice

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 Commission is revising § 318.4(b) to read: "All notifications required under § 318.5(c) (Notice to FTC) involving the unsecured PHR identifiable health information of 500 or more individuals shall be provided contemporaneously with the notice required by

[279] ACLA at 3-4; CTA at 19-21.
[280] 45 CFR §§ 164.400-414.
[281] AdvaMed at 9; AHIP at 7; ACLA at 3; ATA Action at 2; TechNet at 5-6.
[282] ACLA at 3-4.
[283] CTA at 19-21.

§ 318.4(a)." This change requires entities, for breaches involving 500 or more individuals, to notify the FTC consistent with the notice required by § 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. This change also requires that the notice to the FTC be sent at the same time as the notice to the individuals. This requirement thus ensures that the notice to the FTC includes all of the information provided in the notice to the individual. It also avoids a scenario where individuals receive notice before the FTC receives notice and affected individuals contact the FTC about a breach for which the Commission has not been notified.

As a result of this change, the Commission anticipates that entities will have sufficient time to provide complete and fulsome notifications to the Commission. The Commission emphasizes, however, that notice to the FTC should occur "without unreasonable delay," with 60 days serving as the outer limit.[284] The Commission believes that, consistent with public comments, this change effectively harmonizes the notification timeline to the FTC with the notification timeline to the Secretary of HHS under the HIPAA Breach Notification Rule. The Commission also believes that this notification timeline satisfies the Recovery Act requirement that notice be provided "immediately."[285] The Commission also notes that this change does not

[284] As the Commission stated in the 2009 Rule Commentary: "Thus, in some cases, it may be an ''unreasonable delay'' to wait until the 60th day to provide notification. For example, if a vendor of personal health records or PHR related entity learns of a breach, gathers all necessary information, and has systems in place to provide notification within 30 days, it would be unreasonable to wait until the 60th day to send the notice. Similarly, there may be circumstances where a vendor of personal health records discovers that its third party service provider has suffered a breach before the service provider notifies the vendor that the breach has occurred. Indeed, as noted in the text, if the third party service provider is an agent of a vendor of personal health records or PHR related entity, that service provider's knowledge of the breach will be imputed to the vendor of personal health records or PHR related entity. In such circumstances, the vendor should begin taking steps to address the breach immediately, and should not wait until receiving notice from the service provider." 74 FR 42971 n.94 (2009).

[285] 42 U.S.C. 17932(e)(3). Like the Department of Health and Human Services previously concluded with respect to notification to the Secretary under the HIPAA Breach Notification Rule (74 FR 42753 (2009)), the Commission concludes this interpretation satisfies the statutory requirement that notifications of larger breaches be provided to the FTC immediately as compared to the notifications of smaller breaches (i.e., those involving less than 500 individuals), which the statute allows to be reported annually to the FTC.

affect in any way the timing of the notice to the FTC for breaches involving less than 500 individuals.

Finally, a small number of commenters addressed other issues related to timing, such as the timeline for providing notice to consumers or the media. The Commission believes, for the reasons stated in the commentary accompanying the 2009 NPRM and the 2009 Rule Commentary, that the current timelines are appropriate to give consumers and the media timely notice without overburdening notifying firms.[286]

8. Proposed Changes to Improve Rule's Readability

a. The Commission Proposed Changes to Promote Readability

The Commission proposed several changes to improve the Rule's readability. Specifically, the Commission proposed to include explanatory parentheticals for internal cross-references, add statutory citations in relevant places, consolidate notice and timing requirements in single sections, and revise the Enforcement section to state more plainly the penalties for non-compliance.

b. Public Comments Regarding Readability

Commenters supported the Commission's proposed changes to improve the Rule's readability and promote comprehension by including explanatory parentheticals and statutory citations.[287] Commenters also expressed support for the proposed changes to improve the Rule's readability and promote compliance by consolidating into single sections, respectively, the Rule's breach notification and timing requirements.[288] Commenters also favored the proposal to modify § 318.7 to make plain that a violation of the Rule constitutes a violation of a rule

[286] 74 FR 17918 (2009); 74 FR 42971 (2009).
[287] AMA at 6; CARIN Alliance at 9.
[288] AHIMA at 7; AMA at 6-7.

promulgated under section 18 of the FTC Act and is subject to civil penalties, stating that this clarification will decrease the burden on the FTC in enforcement actions and prevent unintended barriers to enforcement.[289]

c. The Commission Adopts Changes Regarding Readability

In light of support from commenters and the Commission's belief that these proposed changes improve readability, the Commission adopts these changes without modification.[290]

III. Paperwork Reduction Act

The Paperwork Reduction Act ("PRA"), 44 U.S.C. chapter 35, requires federal agencies to seek and obtain Office of Management and Budget ("OMB") approval before undertaking a collection of information directed to ten or more persons.[291] This final rule is modifying an

---

[289] AHIMA at 7; AMA at 6-7; AHIOS at 5; MRO at 4. As part of its comment, AMA recommended that the FTC, as Rule violations are filed, use actual examples as case study models for future educational resources. The Commission notes that its existing enforcement actions under the Rule already provide guidance for the marketplace and the FTC also has issued business guidance regarding the Rule. *E.g.,* Fed. Trade Comm'n, *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule* (Sept. 2023), *https://www.ftc.gov/business-guidance/resources/collecting-using-or-sharing-consumer-health-information-look-hipaa-ftc-act-health-breach* (last visited Jan. 11, 2023); Fed. Trade Comm'n, *Health Breach Notification Rule: The Basics for Business* (Jan. 2022), *https://www.ftc.gov/business-guidance/resources/health-breach-notification-rule-basics-business* (last visited Jan. 11, 2024); Fed. Trade Comm'n, *Complying with FTC's Health Breach Notification Rule* (Jan. 2022), *https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0* (last visited Jan. 11, 2024) One commenter also asserted that the Commission was seeking to apply the NPRM's proposed changes retrospectively to breaches of security that were discovered on or after September 24, 2009. This commenter urged the Commission to modify § 318.8 so that the Rule would only apply to breaches of security discovered at least 30 days after the effective date of this Final Rule. TechNet at 5-6. The 2023 NPRM set out the entire part for the convenience of commenters but did not propose any changes to § 318.8. The Commission notes that this effective date section was codified in 2009 when part 318 was added to the CFR and has been in effect since September 24, 2009. As explained in the 2009 Rule Commentary, "the Commission does not have discretion to change the effective date of the rule because the Recovery Act establishes the effective date." See 74 FR 42976; see also 42 U.S.C. 17937(g)(1) ("The provisions of this section shall apply to breaches of security that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations."). The Commission emphasizes that this Final Rule does not apply retroactively.

[290] Relatedly, the Commission also is making a non-substantive grammatical change to § 318.5(a)(2)(ii), which involves substitute notice. This provision currently states: "Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn whether or not the individual's unsecured PHR identifiable health information may be included in the breach." The Commission is revising § 318.5(a)(2)(ii) so it reads: "Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn if the individual's unsecured PHR identifiable health information may have been included in the breach." The Commission made this grammatical change to improve the rule's readability; the change does not alter the provision's substantive meaning.

[291] 44 U.S.C. 3502(3)(A)(i).

existing collection of information,[292] which OMB has approved through July 31, 2025 (OMB Control No. 3084-0150). As required by the PRA, the Commission sought OMB review of the modified information collection requirement at the time of the publication of the NPRM. OMB directed the Commission to resubmit its request at the time the Final Rule is published. Accordingly, simultaneously with the publication of this final rule, the Commission is resubmitting its clearance request to OMB. FTC staff has estimated the burdens associated with the amendments as set forth below.

FTC staff estimates that the amendments to 16 CFR part 318 will likely result in more reportable breaches by covered entities to the FTC. In the event of a breach of security, the covered firms will be required to investigate and, if certain conditions are met, notify consumers, the Commission, and, in some cases, the media.[293]

Based on industry reports, FTC staff estimates that the amendments will cover approximately 193,000 entities, which, in the event that they experience a breach, may be required to notify consumers, the Commission, and, in some cases, the media. While there are approximately 1.8 million apps in the Apple App Store[294] and 2.4 million apps in the Google Play Store,[295] as of March 2024, it appears that roughly 193,000 of the apps offered in either store are categorized as "Health and Fitness."[296]

---

[292] *See* 44 U.S.C. 3502(3)(A)(i).

[293] Third party service providers who experience a breach are required to notify the vendor of personal health records or PHR related entity, which in turn is then required to notify consumers. The Commission expects that the cost of notification to third party service providers would be small, relative to the entities that have to notify consumers. As part of the NPRM, the Commission solicited public comment on this issue and data that may be used to quantify the costs to third party service providers. The Commission did not receive any responsive submissions pertaining to this issue.

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

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

[296] *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

The Commission received three comments in response to the NPRM arguing that the Rule's scope is broader than apps categorized as "Health and Fitness" and that the NPRM's PRA analysis therefore underestimated the number of covered entities and the resulting number of reportable breaches.[297] As discussed above,[298] the Commission is adopting these amendments to clarify that the Rule applies to mobile health applications and similar technologies. The Commission also highlighted several key limitations to the Rule's scope.[299] Thus, the 193,000 covered entities is a rough proxy for all covered PHRs, because it encompasses mobile health applications categorized as "Health and Fitness." Similar health technologies are included in the roughly 193,000 covered entities because most websites and connected health devices that will be covered by the amendments act in conjunction with an app.[300]

FTC staff estimates that these 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 amendments (due to underreporting prior to issuance of the Policy Statement), FTC staff determined the number of estimated breaches by 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

---

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.

[297] *See* Chamber at 2; CHI at 6-7; CCIA at 8-9.

[298] *See* Section II.1.c.

[299] *Id.*

[300] Indeed, one of the commenters who argued that the Rule's coverage is broader than projected in the NPRM's PRA analysis acknowledged that there has been growth in the number of websites and apps since the 2009 PRA analysis estimated 700 covered entities to be covered by the Rule. Chamber at 2. Further, the approximately 193,000 covered entities may overestimate the number of covered entities, as some apps or websites may not qualify as a covered entity given the Rule's boundaries. For example, a website or app must have the technical capacity to draw information from multiple sources and that same website or app must still be "managed, shared, and controlled by or primarily for the individual" to be covered by the Rule.

amendments.[301] Additionally, as the number of breaches per year has grown significantly in the recent years,[302] and FTC staff expects this trend to continue, FTC staff relied on the average number of breaches from 2021 through 2023 to estimate the annual breach incidence rate for HIPAA-covered entities.

Specifically, HHS' OCR reported 715 breaches in 2021, 719 breaches in 2022, and 733 breaches in 2023,[303] 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[304] and the average number of breaches for 2021-2023, 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 (193,000) results in an estimated 82 breaches per year.[305]

---

[301] 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 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.

[302] According to HHS' Office for Civil Rights ("OCR"), the number of breaches per year grew from 276 in 2013 to 739 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.

[303] *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).

[304] 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. 86 FR 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.

[305] One commenter argued that basing the NPRM's projection of the annual number of breaches on the breach incidence rate for HIPAA-covered entities is problematic because the NPRM's proposed definition of a breach of security "goes far and beyond" the HIPAA definition of a breach. CCIA at 8-9. To the extent the commenter is referring to the fact that the Rule's definition of breach of security covers unauthorized disclosures, the Commission notes that the HIPAA Breach Notification Rule similarly covers unauthorized disclosures. *See Breach Notification*

Costs

To determine the costs for purposes of this analysis, FTC staff has developed estimates for two categories of potential costs: (1) the estimated annual burden hours and labor cost of determining what information has been breached, identifying the affected customers, preparing the breach notice, and making the required report to the Commission; and (2) the estimated capital and other non-labor costs associated with notifying consumers.

Estimated Annual Burden Hours: 12,300

Estimated Annual Labor Cost: $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, FTC staff estimates that covered firms will require per breach, on average, 150 hours of employee labor at a cost of $10,770.[306] 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 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).

Estimated Capital and Other Non-Labor Costs: $91,984,370

The capital and non-labor costs associated with breach notifications depend upon the number of consumers contacted and whether covered firms are likely to retain the services of a

Rule, U.S. Dep't of Health & Human Servs., Office for Civil Rights, *https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html* ("A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.")

[306] 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 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*.

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 will spend approximately 40 hours to assist in the response to the cybersecurity intrusion, at an estimated cost of $20,000.[307] 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.[308] 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.[309] This estimate includes the costs of electronic notice, letters, outbound calls or general notice to data subjects; and engagement of

[307] 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).
[308] HHS Breach Data, *supra* note 303. 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.
[309] *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.

outside experts.[310] 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).

FTC staff notes that these estimates likely overstate the costs imposed by the amendments because FTC staff made conservative assumptions in developing many of the underlying estimates. Moreover, many entities covered by the amendments already have similar notification obligations under state data breach laws.[311] In addition, the Commission has taken several steps designed to limit the potential burden on covered entities that are required to provide notice, including by providing exemplar notices that entities may choose to use if they are required to provide notifications and expanding the use of electronic notifications.

IV. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA)[312] requires that the Commission provide an Initial Regulatory Flexibility Analysis ("IRFA") with a proposed rule and a Final Regulatory Flexibility Analysis ("FRFA") with a final rule, unless the Commission certifies that the rule will not have a significant economic impact on a substantial number of small entities. As discussed in the IRFA, the Commission believes that the Final Rule will not have a significant economic impact upon small entities.

---

[310] *See* 2023 IBM Security Report at 72.

[311] Many state data breach notification statutes require notification when a breach occurs involving certain health or medical information of individuals in that state. *See*, *e.g.*, Ala. Code 8-38-1 et seq.; Alaska Stat. 45.48.010 et seq.; Ariz. Rev. Stat. 18-551 et seq.; Ark. Code 4-110-101 et seq.; Cal. Civ. Code 1798.80 et seq.; Cal. Health & Safety Code 1280.15; Colo. Rev. Stat. 6-1-716; Del. Code Ann. tit. 6 12B-101 et seq.; D.C. Code 28-3851 et seq.; Fla. Stat. 501.171; 815 Ill. Comp. Stat. 530/5 et seq.; Md. Code Com. Law 14-3501 et seq; Mo. Rev. Stat. 407.1500; Nev. Rev. Stat. 603A.010 et seq.; N.H. Rev. Stat. 359-C:19– C:21; N.H. Rev. Stat. 332-I:5; N.D. Cent. Code 51-30-01 – 07; Or. Rev. Stat. 646A.600-646A.628; R.I. Gen. Laws 11-49.3-1–11-49.3-6; SDCL 22-40-19 - 22-40-26; Tex. Bus. & Com. Code 521.002, 521.053, 521.151-152; 9 V.S.A. 2430, 2435; Va. Code 18.2-186.6; Va. Code 32.1-127.1:05; Va. Code 58.1-341.2; Wash. Rev. Code 19.255.010 et seq.

[312] 5 U.S.C. 601-612.

In this document, the Commission largely adopts the amendments proposed in its NPRM. The Commission believes that the amendments will not have a significant economic impact upon small entities, although they may affect a substantial number of small businesses. Among other things, the amendments clarify certain definitions, revise the disclosures that must accompany notice of a breach under the Rule, and modernize the methods of notice to allow additional use of electronic notice such as email by entities affected by a breach. In addition, the amendments improve the Rule's readability by clarifying cross-references and adding statutory citations. The Commission does not anticipate that these changes will add significant additional costs for entities covered by the Rule, and by authorizing electronic notice in additional circumstances, the amendments may reduce costs for many entities covered by the Rule. Therefore, the Commission certifies that the amendments will not have a significant economic impact on a substantial number of small entities. Although the Commission certifies under the RFA that the Rule will not have a significant impact on a substantial number of small entities, and hereby provides notice of that certification to the Small Business Administration ("SBA"), the Commission has determined, nonetheless, that it is appropriate to publish an FRFA to inquire into the impact of the proposed amendments on small entities.

A. *Need for and Objectives of the Amendments*

The objective of the amendments is to clarify existing notice obligations for entities covered by the Rule. The legal basis for the amendments is section 13407 of the Recovery Act.

B. *Significant Issues Raised in Public Comments*

Although the Commission received several comments that argued that the amendments would be burdensome for businesses, none argued specifically that smaller businesses in particular would be subject to special burdens. The Commission did not receive any comments filed by the Chief Counsel for Advocacy of the SBA.

C. *Small Entities to Which the Amendments Will Apply*

The amendments, like the current Rule, will apply to vendors of personal health records, PHR related entities, and third party service providers, including developers and purveyors of health apps, connected health devices, and similar technologies. As discussed in the Commission's PRA estimates above, FTC staff estimates that the amendments will apply to approximately 193,000 covered entities. The Commission estimates that a substantial number of these entities likely qualify as small businesses. According to the Statistics on Small Businesses Census data, approximately 94% of "Software Publishers" (the category to which health and fitness apps belong) are small businesses.[313]

D. *Projected Reporting, Recordkeeping, and Other Compliance Requirements, Including Classes of Covered Small Entities and Professional Skills Needed to Comply*

The Recovery Act and the amendments contain certain reporting requirements. The amendments will clarify which entities are subject to those reporting requirements. Specifically, the Act and amendments require vendors of personal health records and PHR related entities to provide notice to consumers, the Commission, and in some cases the media in the event of a breach of unsecured PHR identifiable health information. The Act and amendments also require third party service providers to provide notice to vendors of personal health records and PHR related entities in the event of such a breach. If a breach occurs, each entity covered by the Act and amendments will expend costs to determine the extent of the breach and the individuals affected. If the entity is a vendor of personal health records or a PHR related entity, additional costs will include the costs of preparing a breach notice, notifying the Commission, compiling a list of consumers to whom a breach notice must be sent, and sending a breach notice. Such

[313] *2017 SUSB Annual Data Tables by Establishment Industry*, U.S. Census Bureau (May 2021), *https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html*, using "Data by Enterprise Receipts Size." The U.S. Small Business Administration ("SBA") categorizes Software Publishers as a small business if the annual receipts are less than $41.5 million; the 2017 data is the most recent data available reporting receipts size.

entities may incur additional costs in locating consumers who cannot be reached, and in certain cases, posting a breach notice on a website, notifying consumers through media advertisements, or sending breach notices through press releases to media outlets.

In-house costs may include technical costs to determine the extent of breaches; investigative costs of conducting interviews and gathering information; administrative costs of compiling address lists; professional/legal costs of drafting the notice; and potentially, costs for postage, web posting, and/or advertising. Costs may also include the purchase of services of a forensic expert. As discussed in the context of the PRA, FTC staff estimates that compliance with these requirements will likely result in $883,148 in labor costs and $91,984,370 in capital and other non-labor costs. The estimated cost per covered entity is $481 (the total labor, capital, and non-labor costs of $92,867,518 divided by 193,000 covered entities). The SBA categorizes Software Publishers with annual receipts under $41.5 million as a small business; the per entity cost of $481 represents 0.0001% of this annual receipts threshold.

E. *Significant Alternatives to the Amendments*

In drafting the Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the changes to facilitate electronic notice will assist small entities by significantly reducing the costs of sending breach notices. In addition, the Commission is making available exemplar notices that entities covered by the Rule may use, in their discretion, to notify individuals. The Commission anticipates that these exemplar notices will further reduce the burden on entities that are required to provide notice under the Rule. The Commission is not aware of alternative methods of compliance that will reduce the impact of the amendments on small entities, while also comporting with the Recovery Act. The statutory requirements are specific as to the timing, method, and content of notice.

V. Other Matters

Pursuant to the Congressional Review Act (5 U.S.C. 801 et seq.), the Office of Information and Regulatory Affairs designated this rule as not a "major rule," as defined by 5 U.S.C. 804(2).

List of Subjects in 16 CFR Part 318

Breach,

Consumer Protection,

Health,

Privacy,

Reporting and recordkeeping requirements,

Trade Practices

Accordingly, the Federal Trade Commission amends Title 16, part 318 of the Code of Federal Regulations as follows:

PART 318 – HEALTH BREACH NOTIFICATION RULE

Sec.

318.1 Purpose and scope.
318.2 Definitions.
318.3 Breach notification requirement
318.4 Timeliness of notification.
318.5 Methods of notice.
318.6 Content of Notice.
318.7 Enforcement.
318.8 Effective date.
318.9 Sunset.

Authority: 42 U.S.C. 17937 and 17953.

§ 318.1
Purpose and scope.

(a) This part, which shall be called the "Health Breach Notification Rule," implements section 13407 of the American Recovery and Reinvestment Act of 2009, 42 U.S.C. 17937. It applies to foreign and domestic vendors of personal health records, PHR related entities, and third party

service providers, irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act, that maintain information of U.S. citizens or residents. It does not apply to HIPAA-covered entities, or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity.

(b) This part preempts state law as set forth in section 13421 of the American Recovery and Reinvestment Act of 2009, 42 U.S.C 17951.

§ 318.2
Definitions.

(a) *Breach of security* means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information. A breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure.

(b) *Business associate* means a business associate under the Health Insurance Portability and Accountability Act, Public Law 104–191, 110 Stat. 1936, as defined in 45 CFR 160.103.

(c) *Clear and conspicuous* means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(1) *Reasonably Understandable:* You make your notice reasonably understandable if you:

(i) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(ii) Use short explanatory sentences or bullet lists whenever possible;

(iii) Use definite, concrete, everyday words and active voice whenever possible;

(iv) Avoid multiple negatives;

(v) Avoid legal and highly technical business terminology whenever possible; and

(vi) Avoid explanations that are imprecise and readily subject to different interpretations.

(2) *Designed to call attention.* You design your notice to call attention to the nature and significance of the information in it if you:

(i) Use a plain-language heading to call attention to the notice;

(ii) Use a typeface and type size that are easy to read;

(iii) Provide wide margins and ample line spacing;

(iv) Use boldface or italics for key words; and

(v) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information. The notice should stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

(3) *Notices on websites or within-application messaging.* If you provide a notice on a web page or using within-application messaging, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the website or software application (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(i) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(d) *Electronic mail* means (1) email in combination with one or more of the following: (2) text message, within-application messaging, or electronic banner.

(e) *Health care services or supplies* means any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools.

(f) *Covered health care provider* means a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing health care services or supplies.

(g) *HIPAA-covered entity* means a covered entity under the Health Insurance Portability and Accountability Act, Public Law 104–191, 110 Stat. 1936, as defined in 45 CFR 160.103.

(h) *Personal health record* means an electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

(i) *PHR identifiable health information* means information that:

(1) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

(i) identifies the individual; or

(ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; and

(2) Is created or received by a:

(i) Covered health care provider;

(ii) health plan (as defined in 42 U.S.C. 1320d(5));

(iii) employer; or

(iv) health care clearinghouse (as defined in 42 U.S.C. 1320d(2)); and

(3) with respect to an individual, includes information that is provided by or on behalf of the individual.

(j) *PHR related entity* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that:

(1) Offers products or services through the website, including any online service, of a vendor of personal health records;

(2) Offers products or services through the websites, including any online service, of HIPAA-covered entities that offer individuals personal health records; or

(3) Accesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record.

(k) *State* means any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

(l) *Third party service provider* means an entity that:

(1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and

(2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.

(m) *Unsecured* means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009, 42 U.S.C. 17932(h)(2).

(n) *Vendor of personal health records* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.

§ 318.3
Breach notification requirement.

(a) *In general.* In accordance with § 318.4 (Timeliness of notification), § 318.5 (Methods of notice), and § 318.6 (Content of notice), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each PHR related entity, following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall:

(1) Notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such breach of security;

(2) Notify the Federal Trade Commission; and

(3) Notify prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents

of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(b) *Third party service providers.* A third party service provider shall, following the discovery of a breach of security, provide notice of the breach to an official designated in a written contract by the vendor of personal health records or the PHR related entity to receive such notices or, if such a designation is not made, to a senior official at the vendor of personal health records or PHR related entity to which it provides services, and obtain acknowledgment from such official that such notice was received. Such notification shall include the identification of each customer of the vendor of personal health records or PHR related entity whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, acquired during such breach. For purposes of ensuring implementation of this requirement, vendors of personal health records and PHR related entities shall notify third party service providers of their status as vendors of personal health records or PHR related entities subject to this part. While some third party service providers may access unsecured PHR identifiable health information in the course of providing services, this does not render the third party service provider a PHR related entity.

(c) *Breaches treated as discovered.* A breach of security shall be treated as discovered as of the first day on which such breach is known or reasonably should have been known to the vendor of personal health records, PHR related entity, or third party service provider, respectively. Such vendor, entity, or third party service provider shall be deemed to have knowledge of a breach if such breach is known, or reasonably should have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of such vendor of personal health records, PHR related entity, or third party service provider.

§ 318.4
Timeliness of notification.

(a) *In general.* Except as provided in paragraph (d) of this section (Law enforcement exception), all notifications required under § 318.3(a)(1) (required notice to individuals), § 318.3(b) (required notice by third party service providers), and § 318.3(a)(3) (required notice to media) shall be sent without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security.

(b) *Timing of notice to FTC.* All notifications required under § 318.5(c) (Notice to FTC) involving the unsecured PHR identifiable health information of 500 or more individuals shall be provided contemporaneously with the notice required by § 318.4(a). All logged notifications required under § 318.5(c) (Notice to FTC) involving the unsecured PHR identifiable health information of fewer than 500 individuals may be sent annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year.

(c) *Burden of proof.* The vendor of personal health records, PHR related entity, and third party service provider involved shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

(d) *Law enforcement exception.* If a law enforcement official determines that a notification, notice, or posting required under this part would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed. This paragraph shall be implemented in the same manner as provided under 45 CFR 164.528(a)(2), in the case of a disclosure covered under such section.

§ 318.5
Methods of notice.

(a) *Individual notice.* A vendor of personal health records or PHR related entity that discovers a breach of security shall provide notice of such breach to an individual promptly, as described in § 318.4 (Timeliness of notification), and in the following form:

(1) Written notice at the last known address of the individual. Written notice may be sent by electronic mail if the individual has specified electronic mail as the primary method of communication. Any written notice sent by electronic mail must be Clear and Conspicuous. Where notice via electronic mail is not available or the individual has not specified electronic mail as the primary method of communication, a vendor of personal health records or PHR related entity may provide notice by first-class mail at the last known address of the individual. If the individual is deceased, the vendor of personal health records or PHR related entity that discovered the breach must provide such notice to the next of kin of the individual if the individual had provided contact information for his or her next of kin, along with authorization to contact them. The notice may be provided in one or more mailings as information is available.

(2) If, after making reasonable efforts to contact all individuals to whom notice is required under § 318.3(a), through the means provided in paragraph (a)(1) of this section, the vendor of personal health records or PHR related entity finds that contact information for ten or more individuals is insufficient or out-of-date, the vendor of personal health records or PHR related entity shall provide substitute notice, which shall be reasonably calculated to reach the individuals affected by the breach, in the following form:

(i) Through a conspicuous posting for a period of 90 days on the home page of its website; or

(ii) In major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting shall include a toll-free phone number, which shall remain active for at least 90 days, where an individual can learn if the individual's unsecured PHR identifiable health information may have been included in the breach.

(3) In any case deemed by the vendor of personal health records or PHR related entity to require urgency because of possible imminent misuse of unsecured PHR identifiable health information, that entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (a)(1) of this section.

(b) *Notice to media.* As described in § 318.3(a)(3), a vendor of personal health records or PHR related entity shall provide notice to prominent media outlets serving a State or jurisdiction, following the discovery of a breach of security, if the unsecured PHR identifiable health information of 500 or more residents of such State or jurisdiction is, or is reasonably believed to have been, acquired during such breach.

(c) *Notice to FTC.* Vendors of personal health records and PHR related entities shall provide notice to the Federal Trade Commission following the discovery of a breach of security, as described in § 318.4(b) (Timing of notice to FTC). If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, the vendor of personal health records or PHR related entity may maintain a log of any such breach and submit such a log annually to the Federal Trade Commission as described in § 318.4(b) (Timing of notice to FTC), documenting breaches from the preceding calendar year. All notices pursuant to this paragraph shall be provided according to instructions at the Federal Trade Commission's website.

§ 318.6
Content of notice.

Regardless of the method by which notice is provided to individuals under § 318.5 (Methods of notice) of this part, notice of a breach of security shall be in plain language and include, to the extent possible, the following:

(a) A brief description of what happened, including: the date of the breach and the date of the discovery of the breach, if known; and the full name or identity (or, where providing the full name or identity would pose a risk to individuals or the entity providing notice, a description) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security, if this information is known to the vendor of personal health records or PHR related entity;

(b) A description of the types of unsecured PHR identifiable health information that were involved in the breach (such as but not limited to full name, Social Security number, date of birth, home address, account number, health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, or device identifier (in combination with another data element));

(c) Steps individuals should take to protect themselves from potential harm resulting from the breach;

(d) A brief description of what the entity that experienced the breach is doing to investigate the breach, to mitigate harm, to protect against any further breaches, and to protect affected individuals, such as offering credit monitoring or other services; and

(e) Contact procedures for individuals to ask questions or learn additional information, which must include two or more of the following: toll-free telephone number; email address; website; within-application; or postal address.

§ 318.7
Enforcement.

Any violation of this part shall be treated as a violation of a rule promulgated under section 18 of the Federal Trade Commission Act, 15 U.S.C. 57a, regarding unfair or deceptive acts or practices, and thus subject to civil penalties (as adjusted for inflation pursuant to § 1.98 of this chapter), and the Commission will enforce this Rule in the same manner, by the same means, and with the same jurisdiction, powers, and duties as are available to it pursuant to the Federal Trade Commission Act, 15 U.S.C. 41 *et seq.*

§ 318.8
Effective date.

This part shall apply to breaches of security that are discovered on or after September 24, 2009.

§ 318.9
Sunset.

If new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered by this part, the provisions of this part shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

By direction of the Commission.

April J. Tabor,

Secretary

Note: The following appendix will not appear in the Code of Federal Regulations.

Appendix A: Health Breach Notification Rule Exemplar Notices

The notices below are intended to be examples of notifications that entities may use, in their discretion, to notify individuals of a breach of security pursuant to the Health Breach Notification Rule. The examples below are for illustrative purposes only. You should tailor any notices to the particular facts and circumstances of your breach. While your notice must comply with the Health Breach Notification Rule, you are not required to use the notices below.

Mobile Text Message and In-App Message Exemplars

Text Message Notification Exemplar 1

Due to a security breach on our system, **the health information you shared with us through [name of product] is now in the hands of unknown attackers.** Visit [add non-clickable URL] to learn what happened, how it affects you, and what you can do to protect your information. We also sent you an email with additional information.

Text Message Notification Exemplar 2

You shared health information with us when you used [product name]. **We discovered that we shared your health information with third parties for [describe why the company shared the info] without your permission.** Visit [add non-clickable URL] to learn what happened, how it affects you, and what you can do to protect your information. We also sent you an email with more information.

In-App Message Notification Exemplar 1

Due to a security breach on our system, **the health information you shared with us through [name of product] is now in the hands of unknown attackers.** This could include your [Add specifics – **for example, your name, email, address, blood pressure data**]. Visit [URL] to learn what happened, how it affects you, and what you can do to protect your information. We also sent you an email with additional information.

In-App Message Notification Exemplar 2

You shared health information with us when you used [product name]. **We discovered that we shared your health information with third parties for [if known, describe why the company**

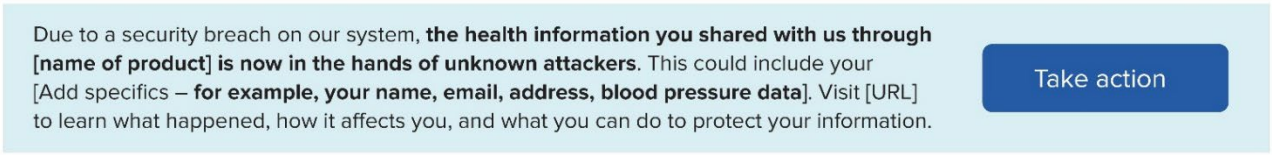
shared the info] without your permission. This could include your [Add specifics – **for example, your name, email, address, blood pressure data**]. Visit [URL] to learn what happened, how it affects you, and what you can do to protect your information. We also sent you an email with additional information.

Web Banner Exemplars

Web Banner Notification Exemplar 1

Due to a security breach on our system, **the health information you shared with us through [name of product] is now in the hands of unknown attackers.** This could include your [Add specifics – **for example, your name, email, address, blood pressure data**]. Visit [URL] to learn what happened, how it affects you, and what you can do to protect your information.

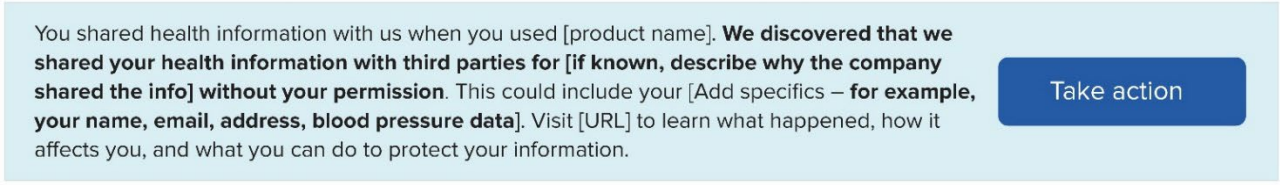
- Recommend: Include clear "Take action" call to action button, such as the example below:



Web Banner Notification Exemplar 2

You shared health information with us when you used [product name]. **We discovered that we shared your health information with third parties for [if known, describe why the company shared the info] without your permission.** This could include your [Add specifics – **for example, your name, email, address, blood pressure data**]. Visit [URL] to learn what happened, how it affects you, and what you can do to protect your information.

- Recommend: Include clear "Take action" call to action button, such as the example below:



Email Exemplars

Exemplar Email Notice 1

Email Sender: [Company] <company email>
Email Subject Line: [Company] Breach of Your Health Information

Dear [Name],

We are contacting you because an attacker recently gained unauthorized access to our system and stole health information about our customers, including you.

What happened and what it means for you
On [March 1, 2024], we learned that an attacker had accessed a file containing our customers' health information on [February 28, 2024]. The file included your name, the name of your health insurance company, your date of birth, and your group or policy number.

What you can do to protect yourself
You can take steps now to reduce the risk of identity theft.

1. **Review your medical records, statements, and bills for signs that someone is using your information.** Under the health privacy law known as HIPAA, you have the right to access your medical records. Get your records and review them for any treatments or doctor visits you don't recognize. If you find any, report them to your healthcare provider in writing. Then go to www.IdentityTheft.gov/steps to see what other steps you can take to limit the damage.

   Also review the Explanation of Benefits statement your insurer sends you when it pays for medical care.

   Some criminals wait before using stolen information so keep monitoring your benefits and bills.

2. **Review your credit reports for errors.** You can get your free credit reports from the three credit bureaus at www.annualcreditreport.com or call 1-877-322-8228. Look for medical billing errors, like medical debt collection notices that you don't recognize. Report any medical billing errors to all three credit bureaus by following the "What To Do Next" steps on www.IdentityTheft.gov.

3. **Sign up for free credit monitoring to detect suspicious activity.** Credit monitoring detects and alerts you about activity on your credit reports. Activity you don't recognize could be a sign that someone stole your identity. We're offering free credit monitoring for two years through [name of service]. Learn more and sign up at [URL].

4. **Consider freezing your credit report or placing a fraud alert on your credit report.** A credit report freeze means potential creditors can't get your credit report without your permission. That makes it less likely that an identity thief can open new accounts in your name. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

   A fraud alert will make it harder for someone to open a new credit account in your name. It tells creditors to contact you before they open any new accounts in your name or change your accounts. A fraud alert lasts for one year. After a year, you can renew it.

   To freeze your credit report, contact **each of the three credit bureaus**, Equifax, Experian, and TransUnion.

   To place a fraud alert, contact **any one of the three credit bureaus**, Equifax, Experian, and TransUnion. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your credit report.

   Credit bureau contact information

   Equifax
   www.equifax.com/personal/credit-report-services
   1-800-685-1111

   Experian
   www.experian.com/help
   1-888-397-3742

   TransUnion
   www.transunion.com/credit-help
   1-888-909-8872

   Learn more about how credit report freezes and fraud alerts can protect you from identity theft or prevent further misuse of your personal information at www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts.

What we are doing in response
We hired security experts to secure our system. We are working with law enforcement to find the attacker. And we are investigating whether we made mistakes that made it possible for the attackers to get in.

Learn more about the breach.
Go to [URL] to learn more about what happened and what you can do to protect yourself. If we have any updates, we will post them there.

If you have questions or concerns, call us at [telephone number], email us at [address], or go to [URL].

Sincerely,

First name Last Name
[Role], [Company]

Exemplar Email Notice 2

Email Sender: [Company] <company email>
Email Subject Line: Unauthorized disclosure of your health information by [Company]

Dear [Name],

We are contacting you because you use our company's app [name of app]. When you downloaded our app, we promised to keep your personal health information private. Instead, we disclosed health information about you without your approval.

What happened?
We told [insert Company name, identity, or, where providing full name or identity would pose a risk to individuals or the entity providing notice, a description of type of company] that you use our app, and between [January 10, 2024] and [March 1, 2024], we gave them your name and your email address.

We gave [insert Company name, identity, or where providing full name or identity would pose a risk to individuals or the entity providing notice, a description of type of company] this information so they could use it for advertising and marketing purposes. For example, to target you for ads for cancer drugs.

What we are doing in response
We will stop selling or sharing your health information with other companies. We will stop using your health information for advertising or marketing purposes. We have asked Company XYZ to delete your health information, but it's possible they could continue to use it for advertising and marketing.

What you can do
We made important changes to our app to fix this problem. Download the latest updates to our app then review your privacy settings. You can also contact Company XYZ to request that it delete your data.

Learn more
Learn more about our privacy and security practices at [URL]. If we have any updates, we will post them there.

If you have any questions or concerns, call us at [telephone number] or email us at [address].

Sincerely,

First name Last Name
[Role], [Company]

Exemplar Email Notice 3

Email Sender: [Company] <company email>
Email Subject Line: [Company] Breach of Your Health Information

Dear [Name],

We are contacting you about a breach of your health information collected through the [product], a device sold by our company, [Company].

What happened? On [March 1, 2024], we discovered that our employee had accidentally posted a database online on [February 28, 2024]. That database included your name, your credit or debit card information, and your blood pressure readings. We don't know if anyone else found the database and saw your information. If someone found the database, they could use personal information to steal your identity or make unauthorized charges in your name.

What you can do to protect yourself
You can take steps now to reduce the risk of identity theft.

1. **Get your free credit report and review it for signs of identity theft.** Order your free credit report at www.annualcreditreport.com. Review it for accounts and activity you don't recognize. Recheck your credit reports periodically.
2. **Consider freezing your credit report or placing a fraud alert on your credit report.** A credit report freeze means potential creditors can't get your credit report without your permission. That makes it less likely that an identity thief can open new accounts in your name. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

   A fraud alert will make it harder for someone to open a new credit account in your name. It tells creditors to contact you before they open any new accounts in your name or change your accounts. A fraud alert lasts for one year. After a year, you can renew it.

   To freeze your credit report, contact **each of the three credit bureaus**, Equifax, Experian, and TransUnion.

   To place a fraud alert, contact **any one of the three credit bureaus**, Equifax, Experian, and TransUnion. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your credit report.

   Credit bureau contact information

Equifax
www.equifax.com/personal/credit-report-services
1-800-685-1111

Experian
www.experian.com/help
1-888-397-3742

TransUnion
www.transunion.com/credit-help
1-888-909-8872

Learn more about how credit report freezes and fraud alerts can protect you from identity theft or prevent further misuse of your personal information at www.consumer.ftc.gov/articles/what-know-about-credit-freezes-and-fraud-alerts.

3. **Sign up for free credit monitoring to detect suspicious activity.** Credit monitoring detects and alerts you about activity on your credit reports. Activity you don't recognize could be a sign that someone stole your identity. We're offering free credit monitoring for two years through [name of service]. Learn more and sign up at [URL].

What we are doing in response
We are investigating our mistakes. We know the database shouldn't have been online and it should have been encrypted. We are making changes to prevent this from happening again.

We are working with experts to secure our system. We are reviewing our databases to make sure we store health information securely.

Learn more about the breach.
Go to [URL] to learn more about what happened and what you can do to protect yourself. If we have any updates, we will post them there.

If you have questions or concerns, call us at [telephone number], email us at [address], or go to [URL].

Sincerely,

First name Last Name
[Role], [Company]