

FEDERAL TRADE COMMISSION

16 CFR Part 318

Health Breach Notification Rule

AGENCY: Federal Trade Commission.

ACTION: Notice of proposed rulemaking; request for public comment.

SUMMARY: The Federal Trade Commission (“FTC” or “Commission”) proposes to amend the Commission’s Health Breach Notification Rule (the “HBN Rule” or the “Rule”) and requests public comment on the proposed changes. 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 would: (1) clarify the Rule’s scope, including its coverage of developers of many health applications (“apps”); (2) amend the definition of breach of security to clarify that a breach of security includes data security breaches and unauthorized disclosures; (3) revise the definition of PHR related entity; (4) clarify what it means for a vendor of personal health records to draw PHR identifiable health information from multiple sources; (5) modernize the method of notice; (6) expand the content of the notice; and (7) improve the Rule’s readability by clarifying cross-references and adding statutory citations, consolidating notice and timing requirements, and articulating the penalties for non-compliance.

DATES: Written comments must be received on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Interested parties may file a comment online or on paper by following the Request for Comment part of the **SUPPLEMENTARY INFORMATION** section below. Write “Health Breach Notification Rule, Project No. P205405” on your comment and file your comment online at <https://www.regulations.gov> by following the instructions on the web-based form. If you prefer to file your comment on paper, mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex H), Washington, DC 20580.

FOR FURTHER INFORMATION CONTACT:

Ryan Mehm (202) 326-2918, Elisa Jillson, (202) 326-3001, Ronnie Solomon, (202) 326-2098, Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

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.

¹ American Recovery and Reinvestment Act of 2009, Public Law No. 111-5, 123 Stat. 115 (2009).

² Health Insurance Portability and Accountability Act, Public Law No. 104-191, 110 Stat. 1936 (1996).

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 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 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 outlets⁶ 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

³ 42 U.S.C. 17937.

⁴ 42 U.S.C. 17921(11).

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 upon what media outlets are “prominent” in the relevant jurisdiction. 74 FR 42974.

⁷ 16 CFR 318.3, 318.5.

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 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 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 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”) and it does not apply to businesses or organizations covered by HIPAA.¹³ HIPAA-covered

⁸ *Id.* 318.3.

⁹ *Id.* 318.4.

¹⁰ *Id.* 318.5(c).

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, Breach Notices Received by the FTC, 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.

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

In May 2020, the Commission announced its regular, ten-year review of the Rule and requested public comments 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.

Many of the commenters encouraged the Commission to clarify that the Rule applies to apps and similar technologies.¹⁸ In fact, no commenter opposed this type of

¹⁴ 45 CFR 164.400-414.

¹⁵ See, e.g., Tehseen Kiani, *App Development in Healthcare: 12 Exciting Facts*, TechnoChops (Jan. 27, 2022), <https://www.technochops.com/programming/4329/app-development-in-healthcare/>; 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>; 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>.

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-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 E.g., Amer. Health Info. Mgmt. Ass’n (“AHIMA”) at 2; Kaiser Permanente at 3; Allscripts at 3; Amer. Acad. of Ophthalmology at 2; All. for Nursing Informatics at 2; Amer. Med. Ass’n (“AMA”) at 4; Amer. College of Surgeons at 6; Physicians’ Elec. Health Record 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.”); America’s

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.¹⁹ Several commenters noted the urgency of this issue, as consumers have further embraced digital health technologies during the COVID-19 pandemic.²⁰ 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 consumers²¹ and to level the competitive playing field among companies dealing with the same health information.²² To that end, commenters not only urged the Commission to revise the Rule, but also to increase its enforcement efforts.²³

1. The Commission’s 2021 Policy Statement

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.

¹⁹ Kaiser Permanente at 7; The Light Collective at 2; Amer. Acad. of Ophthalmology at 2; Healthcare Info. and Mgmt. Sys. Soc’y (“HIMSS”) and the Personal Connected Health All. (“PCH Alliance”) at 3; PEHRC at 2-3.

²⁰ 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 4.

²¹ Georgia Morgan; Amer. Acad. of Ophthalmology at 2-3 (arguing that the breach of health information held by a non-HIPAA-covered app, for example, harms the patient-provider relationship, because the patient erroneously believes that the provider is the source of the breach); 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”).

²² Kaiser Permanente at 2, 4; Workgroup for Electronic Data Interchange (“WEDI”) at 2; AHIP & 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.”).

²³ Kaiser Permanente at 3, 4; Fred Trotter at 1; Casey Quinlan at 1; CARIN All. at 2. At the time of this 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. *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>; *U.S. v. Easy Healthcare Corporation*, Case 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>.

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.²⁴ 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.”²⁵ 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.

The Commission explained that PHR identifiable health information includes individually identifiable health information created or received by a health care provider,²⁶ and that “health care providers” include any entities that “furnish[] health care services or supplies.”²⁷ 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 app makers likely qualify as vendors of personal health records.²⁸

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

²⁴ 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”).

²⁵ 16 CFR 318.2(d).

²⁶ *Id.* 318.2(e).

²⁷ *Id.* 318.2(e); 42 U.S.C. 1320d(6), d(3).

²⁸ *See* Policy Statement at 1.

can be drawn from multiple sources.²⁹ 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;³⁰ a breach is “not limited to cybersecurity intrusions or nefarious behavior.”³¹

2. Enforcement History

In 2023, the Commission has brought its first enforcement actions under the Rule against vendors of personal health records. In February 2023, the Commission brought its first 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.³²

²⁹ 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.

³⁰ 16 CFR 318.2(a).

³¹ Policy Statement at 2; 74 FR 42967 (Commentary to 2009 Final Rule) (“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 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.”) (citations omitted).

³² *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>.

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) to the Federal Trade Commission, or (3) to media outlets. 16 CFR 318.3–6. The Commission entered into a settlement that, among other injunctive relief, required GoodRx to pay a \$1.5 million civil penalty for its violation of the Rule.³³

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

³³ In addition, the Commission alleged that GoodRx’s data sharing practices were deceptive and unfair, in violation of Section 5 of the FTC Act.

notification requirements. The Commission entered into a settlement that, among other injunctive relief, required Easy Healthcare to pay a \$100,000 civil penalty for its violation of the Rule.³⁴

3. Summary of Proposed Rule Changes

Having considered the public comments, described in further detail below, and its Policy Statement, the Commission now proposes to revise the Rule, 16 CFR part 318, in seven ways.

- First, the Commission proposes 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 proposed Rule would modify the definition of “PHR identifiable health information” and add two new definitions (“health care provider” and “health care services or supplies”). These changes are consistent with a number of public comments supporting the Rule’s coverage of these technologies.
- Second, the Commission proposes 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 proposes to revise the definition of PHR related entity in two ways. Consistent with its clarification that the Rule applies to health apps, the Commission first proposes clarifying the definition of “PHR related entity” to make clear that the Rule covers entities that offer products and services through

³⁴ *U.S. v. Easy Healthcare Corporation*, Case 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>.

the online services, including mobile applications, of vendors of personal health records. In addition, the Commission proposes 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 proposes 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 proposes to revise the Rule to authorize electronic notice in additional circumstances. Specifically, the proposed Rule would adjust the language in the “method of notice section” and add a new definition of the term “electronic mail.” The proposed Rule also requires 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.³⁵
- Sixth, the proposed Rule would expand the required content of the notice to individuals, to require that consumers whose unsecured PHR identifiable information has been breached receive additional important information, including information regarding the potential for harm from the breach and

³⁵ 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.

protections that the notifying entity is making available to affected consumers. In addition, the proposed Rule would include 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 proposes to make a number of changes to improve the Rule's readability. Specifically, the Commission proposes 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.

Finally, this Notice also includes a section discussing several alternatives the Commission considered but is not proposing. Although the Commission has not put forth any proposed modifications on those issues, the Commission nonetheless seeks public comment on them.

The Commission believes that the proposed changes are consistent with the language and intent of the Recovery Act, will address the concerns raised by the public comments, and will ensure that the Rule remains relevant in the face of changing business practices and technological developments. The Commission invites comment on the proposed rule revisions generally and on the specific issues outlined through section III. Written comments must be received on or before [INSERT DATE 60 DAYS AFTER PUBLICATION IN THE *FEDERAL REGISTER*].

II. Analysis of the Proposed Rule

The following discussion analyzes the proposed changes to the Rule.

1. Clarification of Entities Covered

The Commission proposes revisions to clarify the Rule’s treatment of health apps and similar technologies not covered by HIPAA. As the Commission’s Policy Statement makes clear, many health apps and similar technologies not covered by HIPAA are covered by the FTC’s existing Rule. To ensure that entities covered by the Rule understand their obligations under the Rule, the Commission is proposing changes to clarify that mobile health applications are covered by the Rule, giving important guidance to the marketplace on the Rule’s scope. To accomplish this objective, the Commission proposes several changes to section 318.2, which defines key terms in the Rule. Commenters broadly support the Rule covering health apps and similar technologies.³⁶

First, consistent with one commenter’s recommendation,³⁷ the Commission proposes revising “PHR identifiable information” to import language from section 1171(6) of the Social Security Act, 42 U.S.C. 1320d(6), which is included in the current Rule only by cross-reference to that statute.³⁸ This revision is not substantive and is being proposed to improve readability.

³⁶ See *supra* note 18.

³⁷ See Lisa McKeen at 5.

³⁸ The HBN Rule, as currently drafted, defines “PHR identifiable health information” as “individually identifiable health information,” as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (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. See 16 CFR 318.2(e). Section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)) states: “The term ‘individually identifiable health information’ means any information, including demographic information collected from an individual, that—

(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(B) 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

As revised, “PHR identifiable information” would be defined 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 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 believes that this 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),³⁹ as well as emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases).⁴⁰ The Commission requests comment as to whether any further amendment of the definition is needed to clarify the scope of data covered.

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

³⁹ *In the Matter of Flo Health, Inc.*, FTC File No. 1923133 (June 22, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc.>; *In the Matter of BetterHelp, Inc.*, FTC File No. 2023169 (March 2, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter> (proposed complaint and order); *U.S. v. Easy Healthcare Corporation*, Case 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.>; *See also* U.S. Dep’t of Health & Human Servs., *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

⁴⁰ *See e.g.*, Mason Marks, *Emergent Medical Data: Health Information Inferred by Artificial Intelligence*, 11 UC Irvine L. Rev. 995 (2021), <https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1501&context=ucilr>.

The proposed Rule also defines a new term, “health care provider,” in a manner similar to the definition of “health care provider” found in 42 U.S.C. 1320d(3) (and referenced in 1320d(6)). Specifically, the proposed Rule defines “health care provider” to mean a provider of services (as defined in 42 U.S.C. 1395x(u)⁴¹), 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 proposed Rule adds a new definition for the term “health care services or supplies” 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.⁴² The Commission’s proposed definition of “health care services and supplies” is based on a number of factors, including the Commission’s institutional knowledge, expertise, and law enforcement experience in health data technology. This definition is designed to reflect the current state of technology for health apps and connected devices, as well as emerging

⁴¹ Under 42 U.S.C. 1395x(u), the term “provider of services” means a hospital, critical access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1395f(g) and section 1395n(e) of this title, a fund.

⁴² See Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter, Concurring in Part, Dissenting in Part, *In the Matter of Flo Health, Inc.*, FTC File No. 1923133 (Jan. 13, 2021), https://www.ftc.gov/system/files/documents/public_statements/1586018/20210112_final_joint_rerks_statement_on_flo.pdf (“The FTC’s Health Breach Notification Rule covers (a) health care providers that (b) store unsecured, personally identifiable health information that (c) can be drawn from multiple sources, and the rule is triggered when such entities experience a ‘breach of security.’ See 16 CFR 318. Under the definitions cross-referenced by the Rule, Flo – which markets itself as a ‘health assistant’ – is a ‘health care provider,’ in that it ‘furnish[es] health care services and supplies.’ See 16 CFR 318.2(e); 42 U.S.C. 1320d(6), d(3).”).

technological capabilities that the Commission has observed through its investigatory, enforcement, and policy work.

These changes clarify that developers of health apps and similar technologies providing these types of “health care services or supplies” qualify as “health care providers” under the Rule. Accordingly, any individually identifiable health information these products collect or use would constitute “PHR identifiable health information” covered by the Rule. These changes also clarify that mobile health applications, therefore, are a “personal health record” covered by the Rule (as long as other conditions set forth in the definition of “personal health record” are met) and accordingly the developers of such applications are “vendors of personal health records.”⁴³ The proposed definition of “health care services or supplies” clarifies the Rule’s scope in two ways. First, it makes clear that the Rule applies generally to online services, including websites, apps, and Internet-connected devices that provide health care services or supplies. Second, it illustrates 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 intends to ensure app developers understand their notice obligations, even if an app is positioned as a “wellness” product rather than a “health” product.

⁴³ The mobile health applications covered as “vendors of personal health records” under the Rule are distinct from the “online applications” referenced in footnote 78 of the 2009 Statement of Basis and Purpose as “PHR related entities.” Footnote 78 from the 2009 Statement of Basis and Purpose states that PHR related entities include “online applications through which individuals connect their blood pressure cuffs, blood glucose monitors, or other devices” so they can track the results through their personal health records. *See* 74 FR 42962, 42969 n.78 (2009). Footnote 78 refers narrowly to online applications that collect health information from a single source and transfer it to a personal health record maintained separate and apart from the PHR related entity by the PHR vendor. In other words, a PHR related entity sends health information to a personal health record which the PHR related entity does not itself maintain.

The Commission’s proposed changes are consistent with the public comments, which recommended the Rule cover health apps and similar technologies.⁴⁴ In revising and adding these definitions, Commission staff also sought informal input from staff at the federal agencies that interpret or enforce the referenced statutory provision, 42 U.S.C. 1320d, including staff at HHS. The Commission’s definition of “health care provider” differs from, but does not contradict, the definitions or interpretations adopted by HHS.⁴⁵ The Commission’s proposed definition is consistent with the statutory scheme established by Congress to regulate non-HIPAA covered entities and within the agency’s discretion in administering the Rule.

Topics on Which the Commission Seeks Public Comment

The Commission seeks comment as to whether these changes sufficiently clarify the Rule’s application to purveyors of health apps and similar technologies that are not covered by HIPAA. The Commission also seeks comment as to whether the proposed rule, as explained here, makes clear to the market which entities are covered by the Rule and under what circumstances. As the Commission has explained, the Rule is intended to cover developers and purveyors of health apps and Internet-connected health devices, such as fitness trackers, that are not covered by HIPAA. The Commission seeks comment as to whether the proposed changes and added definitions would apply to entities that offer other technologies and, if so, whether these definitions include appropriate distinctions. If the scope should be limited, the Commission seeks comment as to how

⁴⁴ See *supra* note 18.

⁴⁵ Although in other contexts HHS has defined the term “health care provider” based upon a more limited understanding of that term (e.g., referring primarily to persons and entities such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies), its definition does not contradict or preclude an interpretation of the referenced statutory provision, 42 U.S.C. 1320d, that encompasses developers of health applications and similar technologies.

that limitation could be effected through the Rule’s language, consistent with the language and purpose of the Recovery Act. The Commission seeks comment on defining “health care provider” in a manner that is broader than a more limited definition of that term used in other contexts (e.g., referring primarily to persons and entities such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies⁴⁶). And, finally, the Commission seeks comment on the definition of “healthcare services or supplies,” including whether any modifications should be made to this definition.

2. Clarification Regarding Types of Breaches Subject to the Rule

The Commission proposes 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 current Rule defines “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.⁴⁷ This language mirrors the definition of “breach of security” in section 13407(f)(1) of the Recovery Act. The current Rule also includes a rebuttable presumption for unauthorized access to an individual’s data. It states that when there is unauthorized access to data, unauthorized acquisition will be presumed unless the entity that experienced the breach “has reliable

⁴⁶ See, e.g., U.S. Dep’t of Human Servs., Guidance on Covered Entities and Business Associates (June 16, 2017), <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html> (listing these persons/entities as examples of health care providers).

⁴⁷ 16 CFR 318.2(a).

evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.”⁴⁸

The Commission’s proposed changes are consistent with the plain language of the current Rule and the Recovery Act definition of “breach of security.”⁴⁹ Additionally, 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.”⁵⁰ Further, recent Commission enforcement actions against *GoodRx* and *Easy Healthcare* also make clear that the Rule covers unauthorized disclosures of consumers’ PHR identifiable health information to third party companies. The Commission’s proposed changes also are consistent with public comments, which urged the Commission to clarify what constitutes an unauthorized acquisition under the Rule.⁵¹

Accordingly, consistent with the Recovery Act definition, the Policy Statement, FTC enforcement actions under the Rule, and public comments received, the

⁴⁸ 16 CFR 318.2(a).

⁴⁹ The commentary to the current Rule already provides guidance on the types of disclosures that the Commission considers to be “unauthorized.” For instance, it states: “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.” 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.

⁵⁰ Policy Statement at 2.

⁵¹ See 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 individual the specific secondary recipients of the individual’s data.”); Amer. Med. Informatics Ass’n (“AMIA”) at 2 (recommending that the FTC “[e]xpand on the concept of

Commission proposes amending the definition of “breach of security” in section 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 proposed definition is 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.

Topics on Which the Commission Seeks Public Comment

The Commission seeks comment on (1) whether this addition to the definition of “breach of security” is necessary, given that the definition in the current Rule already encompasses unauthorized acquisitions beyond security breaches, and (2) whether the proposed definitional change sufficiently clarifies for the marketplace the Rule’s coverage.

3. Revised Scope of PHR related entity

The Commission also proposes revising the definition of “PHR related entity” in two ways that pertain to the Rule’s scope. Currently, the Rule defines “PHR related entity” to mean an entity, other than a HIPAA-covered entity or a business associate of a HIPAA-covered entity, that: (1) offers products or services through the website of a

‘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.).

vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals personal health records; or (3) accesses information in a personal health record or sends information to a personal health record.⁵²

First, the Commission proposes language to clarify that 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. Commenters urged this change because websites are no longer the only means through which consumers access health information online.⁵³ To the contrary, online services such as apps are equally relevant to consumers' online experiences with health information.

Second, the Commission proposes to revise the third prong of the definition so 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 — qualify as PHR related entities. This change — from *any* information to *unsecured PHR identifiable health information* — is intended to eliminate potential confusion about the Rule's breadth and promote compliance by narrowing the

⁵² 16 CFR 318.2(f).

⁵³ See, e.g., AHIMA at 2 (“[W]e also recommend that the Commission consider updating the existing definition of a ‘PHR-related entity’ [sic] at 318.2(f) as 318.2(f)(1) and 318.2(f)(2) appear to focus primarily on products and services offered through a vendor’s website and may not be entirely reflective of today’s environment as new platforms and related services are increasingly deployed and adopted.”; Amer. Acad. of Ophthalmology at 3–4 (recommending that the definition cover apps); PEHRC at 4 (same).

scope of entities that qualify as PHR related entities.⁵⁴

As the Rule is currently drafted, for example, a grocery delivery service that integrates with a diet and fitness app could arguably be considered a PHR related entity when the grocery delivery service sends information about food purchases to the diet and fitness app. This expansive reading of the Rule is not consistent with the purposes of the statute or the Commission's intent when it drafted the Rule. The Commission believes that a more appropriate interpretation of the term PHR related entity encompasses entities that access *unsecured PHR identifiable health information* in a personal health record or send *unsecured PHR identifiable health information* to a personal health record. Remote blood pressure cuffs, connected blood glucose monitors, and fitness trackers are all

⁵⁴ The revised definition would state 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 nevertheless believes 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, under the Rule's current formulation, 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 this proposed revision, does not qualify as a PHR related entity in the first place, there is no need to consider whether it experienced a reportable breach.

examples of devices that could qualify as a PHR related entity when individuals sync them with a personal health record (i.e., mobile health application).⁵⁵

As a result of this proposed change, a firm that performs attribution and analytics services for a health app might 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. This overlap could create competing notice obligations, where, in the event of a breach, the firm would be required to notify individuals and the FTC (per section 318.3's notice requirements for PHR related entities) *and* notify the vendor of the personal health record (per section 318.3's notice requirements for third party service providers).

The Commission does not intend this result. Instead, the Commission considers firms that perform services such as attribution and analytics for apps and technologies providing healthcare services and supplies to be third party service providers. Such service providers must notify the health app developers for whom they provide services, who in turn would notify affected individuals.⁵⁶ Otherwise, treating such service providers as PHR related entities would create a problematic result for the consumer, who would receive notice from an unfamiliar company. To clarify this issue, the Commission

⁵⁵ 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). 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).

⁵⁶ In attempting to help distinguish between PHR related entities and third party service providers, the Commission offers the following observation: in most cases, third party service providers are likely to be non-consumer facing. Thus, examples of PHR related entities include, as noted above, fitness trackers and health monitors when consumers sync them with a mobile health app. Examples of third party service providers include entities that provide support or administrative functions to vendors of personal health records and PHR related entities.

proposes to revise section 318.3(b) by adding 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.

Moreover, this result will create incentives for responsible data stewardship and for de-identification. Specifically, PHR vendors will have incentives to select and retain service providers, such as those that perform services such as attribution or analytics for apps, capable of treating data responsibly (e.g., not engaging in any onward disclosures of data that could result in a reportable breach) and incentives to oversee their service providers to ensure ongoing responsible data stewardship (which would avoid a breach). Further, it will create incentives for PHR vendors to avoid breaches by service providers by de-identifying health information *before* sharing it with any service provider, as de-identification would render the data no longer PHR identifiable health information subject to the Rule.

a. Topics on Which the Commission Seeks Public Comment

The Commission seeks comment on whether additional changes to the Rule would be necessary or helpful to clarify this result. The Commission also requests comment on the following scenario: a third party service provider, such as an analytics firm, receives PHR identifiable health info (e.g., device identifier and geolocation data from which health information about an individual can be inferred) and then sells it to another entity without the consumer's authorization. The Commission considers this to be a reportable breach, even if the consumer consented to the original collection. In such a scenario, the third party service provider would be required to notify the vendor of personal health records or PHR related entity, who in turn would notify affected

individuals. The Commission requests comment on this approach, including whether as a policy matter it is advisable under the Rule to require a vendor of personal health records or PHR related entity to notify its customers about such onward disclosures.

The Commission also seeks comment on the definition of “PHR related entity,” including the scope. Conversely, the Commission seeks comment as to whether, by limiting the third prong of the definition to entities that access or send unsecured PHR identifiable health information, the proposed definition is too narrow and would exclude entities that should be required to notify consumers of breaches, consistent with the Recovery Act. To assess this question of breadth, the Commission requests comment on what entities are (1) offering products or services through personal health records such as apps; or (2) sending or accessing information, including but not limited to identifiable health information, in health apps and other personal health records. Finally, the Commission requests comment on the potential overlap between the definitions of “PHR related entity” and “third party service provider,” and how to sufficiently distinguish between them.

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

The Commission proposes revising the definition of “personal health record” to clarify what it means for a personal health record to draw information from multiple sources. Under the current 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.

Under the revised 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.⁵⁷

This change clarifies the application of the statutory definition of a personal health record that can draw information from multiple sources. Adding the phrase “technical capacity to draw information” 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 from 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” would clarify that a product is a personal health record if it can draw *any* information from multiple sources, even if it only draws *health*

⁵⁷ One commenter specifically recommended that the definition of PHR be broadened to “to explicitly include any website, mobile application, or other electronic record system that collects and stores individually identifiable information, including health information, even if it draws that information from a single source.” Kaiser Permanente at 3.

information from one source. This change further clarifies the Commission’s interpretation of the Recovery Act, as explained in the Policy Statement.⁵⁸

To illustrate the intended meaning of the proposed revisions to the term “personal health record,” the Commission offers the example of two non-HIPAA covered diet and fitness apps available for consumer download in an app store. The proposed Rule makes clear that each is a personal health record.

- Diet and Fitness App Y allows users to sync their app with third-party wearable fitness trackers with the app. Diet and Fitness App Y has the technical capacity to draw identifiable health information both from the user (name, weight, height, age) and the fitness tracker (user’s name, miles run, heart rate), even if some users elect not to connect the fitness tracker.
- 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 (name, weight, height, age) and non-health information (calendar entry info, location, and time zone) from the user’s calendar.

a. Topics on Which the Commission Seeks Public Comment

The Commission seeks comment as to whether the proposed changes sufficiently clarify the Rule’s application to developers and purveyors of products that have the technical capacity to draw information from more than one source. In particular, the Commission invites 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

⁵⁸ Policy Statement at 2.

particular users of the app choose not to enable the syncing features. The Commission also requests 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 also requests 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. For example, an app 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. The Commission also requests comment on the likelihood of such scenarios.

5. Facilitating Greater Opportunity for Electronic Notice

Fourth, the Commission proposes to authorize expanded use of email and other electronic means of providing clear and effective notice of a breach to consumers. Increasingly, consumers interact with vendors of personal health records (and vice versa) solely online and communicate primarily or exclusively through electronic means.

Currently, the Rule permits notice by either postal mail or, in limited circumstances, email. The Rule provides that vendors of personal health records or PHR related entities that discover a breach of security must provide “[w]ritten notice, by first-class mail to the individual at the last known address of the individual, or by email, if the

individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice.”⁵⁹

Several commenters noted the cost and inconvenience associated with postal mail notice to companies and consumers alike.⁶⁰ Several commenters encouraged the Commission to update the methods of notice to permit notice by electronic means.⁶¹ Commenters suggested that the Commission revise the Rule to encourage different kinds of electronic notice, including email, in-app messaging, and QR codes.⁶² For example, one commenter stated that the Rule’s notice requirement should be updated to permit notification by email or within an application, including through such means as banner, “pop-up,” and clickthrough notifications.⁶³ This commenter also noted that an electronic communication is more likely to be read by an individual who is using an application, and is more cost effective.⁶⁴ Another commenter urged the Commission to increase the options for breach notification to include email rather than certified mail as the only option.⁶⁵ And another commenter noted that in-app messaging, text messages, and platform messaging are widely used tools and should be allowed to be utilized to more effectively communicate with consumers that consent to them.⁶⁶ This commenter added that it is common sense that consumers should be able to consent to receiving communications under the Rule via these modalities as well as via email.⁶⁷

⁵⁹ 16 CFR 318.5(a)(1).

⁶⁰ Allscripts at 2; Bruce Grimm at 1; All. for Nursing Informatics at 2; Anonymous, No. FTC-2020-0045-0005 at 1; CHI at 3; CARIN All. at 2.

⁶¹ The App Ass’n’s Connected Health Initiative (“CHI”) at 3; CARIN All. at 2; Allscripts at 2; Bruce Grimm at 1; All. for Nursing Informatics at 2.

⁶² *Id.*

⁶³ Allscripts at 2.

⁶⁴ *Id.*

⁶⁵ All. for Nursing Informatics at 2.

⁶⁶ CHI at 3.

⁶⁷ *Id.*

The Commission recognizes that, as commenters noted, the relationship between vendors of personal health records and PHR related entities, on the one hand, and individuals takes place online and increasingly via applications present on devices such as mobile phones and tablets. These applications communicate with individuals by various electronic means, including text, within-application message, and email.

a. Notice via Electronic Mail

Accordingly, the Commission proposes to update this provision 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 and 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.

Authorizing entities to provide notice about a breach of security by electronic mail is consistent with how consumers often receive other communications from these entities and will align with consumers' expectations. As a result, they are less likely to be ignored or viewed as suspicious by individuals.

Consistent with this objective, the Commission proposes defining "electronic mail" to mean email in combination with one or more of the following: text message, within-application messaging, or electronic banner. The proposed Rule would facilitate more notice by electronic mail. This new definition of electronic mail would ensure that the notice is both (1) convenient and low-cost (because it is electronic) and (2) unavoidable and consistent with the consumer's relationship with the product. For example, if an app developer is providing notice, it could send written notice by email and in-app message, ensuring that the consumer receives notice in a manner consistent

with her experience with the app. Similarly, a website operator could send written notice by email and an electronic banner on the home page of its website. The two prongs of the definition would ensure that a notifying entity cannot select a single form of electronic notice that is unlikely to reach consumers — for example, sending an in-app message alone to app users who do not frequently check in-app notifications.

The goal of structuring the notice in two parts is to increase the likelihood that consumers encounter the notice. Many individuals routinely check email messages, making email a useful vehicle to communicate a breach notification. However, some individuals do not read email often, and these consumers under the proposed definition would also receive notice via text, in-app, or banner notice, thereby increasing the likelihood that they will encounter the breach notification.

The Commission believes any notification delivered via electronic mail should be clear and conspicuous. The proposed Rule defines “clear and conspicuous.” Among other things, for a notice to be clear and conspicuous, the notice must be reasonably understandable and designed to call attention to the nature and significance of the information in the notice. The proposed definition of “clear and conspicuous” closely tracks the definition of clear and conspicuous in the FTC’s Financial Privacy Rule.⁶⁸

Vendors of personal health records and PHR related entities must obtain consumer consent prior to adopting “electronic mail” as their notification method for affected individuals. The proposed Rule would require that entities covered by the Rule may provide “electronic mail” notifications if the individual user has specified electronic mail as their primary method of communication with the entity. This is consistent with

⁶⁸ 16 CFR 313.3(b)(1).

section 13402 of the Recovery Act, which requires that entities can only send notice by electronic mail “if specified as a preference by the individual.” The Commission interprets this phrase as allowing entities to send an email or in-app alert notifying their users that they will receive breach notices by electronic mail and offering them the opportunity to opt out of electronic mail notification and instead receive notice by first class mail. The proposed Rule also allows for notification by first-class mail where electronic mail is not available.

b. Model Notice

To assist entities that are required to provide notice to individuals under the Rule, the Commission has developed a model notice that entities may use, in their discretion, to notify individuals. This model notice is attached as Exhibit A to this Notice of Proposed Rulemaking. The Commission invites comment on this model notice, including: (1) whether the model notice should be mandatory and any advantages or disadvantages of mandating use of the model notice; (2) whether and how the model notice could be compatible with the methods of notice contemplated by the proposed definition of electronic mail, such as text, banner and within-application messaging, including whether and how entities could suitably link to model notice language from a text message,⁶⁹ electronic banner, or in-application message; (3) and recommended changes to the substance and format of the model notice.

⁶⁹ The proposed text message and in-app language in the exemplar notice invites consumers to “Visit [add non-clickable URL] to learn what happened, how it affects you, and what you can do to protect your information.” The exemplar proposes a non-clickable URL due to the risk that a clickable URL could expose consumers to, for example, malware or scams.

c. Topics on Which the Commission Seeks Public Comment

The Commission also requests comment on the proposed changes, including whether the definition of “electronic mail” would achieve the Commission’s goal to make notice unavoidable and consistent with the consumer’s relationship with the product. The Commission also requests comment as to whether this definition would result in over-notification from “duplicate” notices, including the extent to which the proposed two-pronged approach could confuse consumers or reduce the impact that a single notice might have. And the Commission requests comment as to whether this definition is consistent with principles of data minimization, i.e., whether an entity might collect more data (e.g., email or text) than it otherwise would have simply to obtain sufficient information to send notice via “electronic mail” in the event of a breach.

6. Expanded Content of Notice

The Commission proposes several modifications to the content of the required notice to individuals. Currently, the Rule requires that the notice include a description of what happened; a description of the types of unsecured PHR identifiable health information that were involved in the breach; the steps individuals should take to protect themselves from potential harm; a description of what the vendor of personal health records or PHR related entity involved is doing to investigate the breach, to mitigate any losses, and to protect against any further breaches; and contact procedures for individuals to ask questions or learn additional information.⁷⁰ The Commission proposes five changes to the content of the notice.

⁷⁰ 16 CFR 318.6.

a. Summary of Changes to Content of the Notice

First, in section 318.6(a), as part of relaying what happened regarding the breach, the Commission proposes 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.

The Commission proposes adding this provision so that individuals better understand the nexus between the information breached and the potential harms that could result from the breach of such information. In some cases, it is unclear to individuals what harms may flow from the breach of their information. The Commission believes it is important to equip individuals with information about the harms they may experience so that they can better understand the potential risks from a breach and determine what steps or measures to take following a breach. The Commission invites comment on this proposed provision, including (1) whether the requirement that the notice describe potential harms would serve the public interest and benefit consumers, (2) whether notifying entities typically possess information following a breach to assess the potential harms to individuals, (3) whether, in the absence of such information, notifying entities may minimize the potential risks by informing individuals that they are unaware of any harms that may result from the breach, (4) how notifying entities, in the absence of known, actionable harm resulting from a breach, should best describe to individuals the potential harms they may experience, and (5) whether additional and more specific data elements may overwhelm or confuse recipients of the notice.

Second, the Commission also proposes to amend the requirements for the notice under section 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, 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). No such requirement exists in the current Rule.

Third, the Commission proposes modifications to section 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 Rule currently sets forth examples of different types of PHR identifiable health information, such as full name, date of birth, Social Security number, account number, or disability code, that could have been involved in the breach.

The Commission proposes 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. The Commission believes it is important for individuals 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.⁷¹ For example, even the disclosure of an individual's use of a health-related mobile application (e.g., a HIV management app, mental health app, or addiction recovery app) could, depending on the type of health app at issue, lead to a

⁷¹ See, e.g., Fed. Trade Comm'n, FTC Informational Injury Workshop: BE and BCP Staff Perspective (Oct. 2018), https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf; Fed. Trade Comm'n, Former Acting Chairwoman Maureen K. Ohlhausen, *Painting the Privacy Landscape: Informational Injury in FTC Privacy and Data Security Cases* (Sept. 19, 2017), https://www.ftc.gov/system/files/documents/public_statements/1255113/privacy_speech_mkohlhausen.pdf.

number of potential injuries, including embarrassment, social stigma, more expensive health insurance premiums, or even loss of employment.

Fourth, section 318.6(d) of the Rule currently requires that a vendor of personal health records or PHR related entity describe what the entity is doing to investigate the breach, to mitigate any losses, and to protect against any further breaches. The Commission proposes to revise this provision 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. The Commission believes it is important that notifying entities explain to individuals not only the steps individuals should take to protect themselves from potential harm resulting from the breach, but also what steps the notifying entity is taking to protect affected individuals following the breach. Any protections offered by notifying entities likely will be tailored to the facts and circumstances of each breach and could, in certain circumstances, include credit monitoring or other support such as identity theft protection or identity restoration services.

Fifth, the Commission proposes to modify section 318.6(e). Currently, this section requires that the notice to individuals include contact procedures for individuals to ask questions or learn additional information about the breach, and the contact procedure must include one of the following: a toll-free telephone number; an email address; website; or postal address. The Commission proposes to modify section 318.6(e) to specify 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. The Commission proposes this change to encourage and facilitate communication between the notifying entities and affected individuals. This modification is intended to avoid a scenario where, for example, a notifying entity regularly communicates with most of its customers via email and the notifying entity establishes a postal address as the only contact procedure for individuals to employ following a breach.

7. Proposed Changes to Improve Rule's Readability

The Commission proposes several changes to improve the Rule's readability. Specifically, the Commission proposes 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.

a. Explanatory Parentheticals and Statutory References

Throughout the Rule, the Commission proposes to include explanatory parentheticals for each internal cross-reference and add statutory citations to help orient the reader.⁷² The Commission invites comment on whether the inclusion of explanatory

⁷² For example, the Commission proposes to add a statutory citation for the Recovery Act section referenced in the definition of "unsecured," to improve the clarity and readability of this defined term. The revised definition would provide that "unsecured" means PHR identifiable health 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).

parentheticals and statutory citations improves the Rule’s readability and promotes comprehension.

(1) Consolidated Notice and Timing Requirements

To facilitate reader understanding, the Commission proposes consolidating into single sections, respectively, the Rule’s breach notification and timing requirements. Currently, the breach notification requirements are located in sections 318.3 and 318.5 and the timing requirements are located in sections 318.4 and 318.5.

To consolidate the Rule’s notice requirements, the Commission proposes to move the provision in section 318.5 (Methods of notice) requiring notice to the media (section 318.5(b)) to section 318.3. The Commission does not intend to make any substantive change to the breach notification requirements; this change is merely intended to consolidate breach notification requirements in a single section to improve readability and promote compliance.

New subsection 318.3(a)(3) would set forth the requirement to notify prominent media⁷³ 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. The Commission requests comment as to whether the consolidation of breach notification requirements improves the Rule’s readability and will promote compliance.⁷⁴

⁷³ See *supra* note 6.

⁷⁴ As noted above, the Commission does not intend this consolidation of timing requirements to have any effect on the substantive requirements of the Rule. In making this proposed change, minor revisions are required to section 318.5(b). Section 318.5(b) of the proposed Rule would provide: “*Notice to media.* As described in section 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.”

Second, to consolidate requirements regarding the timing of notification, the Commission proposes moving timing requirements for notice to the FTC that appear in section 318.5(c) of the current Rule to a new subsection (b) in section 318.4 of the proposed Rule. Accordingly, proposed section 318.4(b) would now require vendors of personal health records and PHR related entities to notify the Commission as soon as possible and in no case later than ten business days following the date of discovery of the breach if the breach involves the unsecured PHR identifiable health information of 500 or more individuals. If the breach involves the unsecured PHR identifiable health information of fewer than 500 individuals, this section permits vendors of personal health records and PHR related entities, in lieu of immediate notice, to maintain a breach log and submit this log annually to the Federal Trade Commission no later than 60 calendar days following the end of the calendar year.⁷⁵

Importantly, the Commission does not intend to make any substantive change to the timing requirements; this change is merely intended to consolidate timing requirements in a single section to improve readability and promote compliance. The Commission requests comment as to whether the inclusion of explanatory parentheticals and the proposed consolidation of timing requirements improves the Rule's readability and will promote compliance.

⁷⁵ As noted above, the Commission does not intend this consolidation of timing requirements to have any effect on the substantive requirements of these sections. Section 318.5(c) of the proposed Rule would provide: "(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 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."

(2) Revised Enforcement Provision

Commenters suggested that the Rule be revised to specify the penalties for non-compliance.⁷⁶ Currently, the Rule provides that a violation of section 318.3 shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18 of the FTC Act. The Commission proposes modifying section 318.7 to make plain that a violation of the Rule constitutes a violation of a rule promulgated under section 18 of the FTC Act and is subject to civil penalties.

Under section 18 of the FTC Act, 15 U.S.C. 57a, the Commission is authorized to prescribe “rules which define with specificity acts or practices which are unfair or deceptive acts or practices in or affecting commerce” within the meaning of section 5(a)(1) of the FTC Act, 15 U.S.C. 45(a)(1). Once the Commission has promulgated a trade regulation rule, anyone who violates the rule with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such act is unfair or deceptive and is prohibited by such rule is liable for civil penalties for each violation. 15 U.S.C. 45(m)(1)(A). Entities that fail to comply with the Rule are subject to penalties of up to \$50,120 per violation per day, and this amount is increased annually per the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015.⁷⁷ The Commission seeks comment on these proposed modifications to section 318.7.

⁷⁶ See Bruce Grimm at 1 (“Areas of 16 CFR [p]art 318.5 method of notice could be enhanced by adding an option for consumers to text or use a quick response (QR) code generator to obtain data breach information that is on file. This coupled with a modification of 16 CFR [p]art 318.7 enforcement where the actual potential penalty for practice in violation of regulation is noted would act as a deterrent to non-compliance.”); All. for Nursing Informatics at 2 (“We offer the following additional considerations to update and improve the HBN Rule, including. . . . Identify sufficiently stringent penalties and monitoring for responsible management of identifiable PHI.”).

⁷⁷ 16 CFR 1.98; see also Federal Trade Commission, *FTC Publishes Inflation-Adjusted Civil Penalty Amounts for 2022* (Jan. 6, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts-2023>.

III. Changes Considered but not Proposed and on Which the Commission Seeks Public Comment

1. Defining Authorization and Affirmative Express Consent

As previously noted above, when a health app or other device discloses sensitive health information without users' authorization, this is a "breach of security" under the Rule. The Commission considered defining the term "authorization," which appears in section 318.2(a)'s definition of "breach of security." Specifically, section 318.2(a) defines "breach of security," in relevant part, to mean the acquisition of unsecured PHR identifiable information of an individual in a personal health record without the "authorization" of the individual. 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).⁷⁸ Such changes would ensure that notification is required anytime there is acquisition of unsecured PHR identifiable information without the individual's affirmative express consent for that acquisition—such as when an app discloses unsecured PHR identifiable information to another

⁷⁸ 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.

company, having obtained nominal “consent” from the individual by using a small, greyed-out, pre-selected checkbox following a page of dense legalese.

In considering whether to define “authorization” and “affirmative express consent,” the Commission considered public comments that argued the Rule should do more to prevent data collection and use without the individual’s consent.⁷⁹ Defining these terms to emphasize the importance of meaningful consent would partially address the concerns of some commenters that privacy compliance obligations for entities not covered by HIPAA should be similar to obligations for HIPAA covered entities, both to ensure consistent protections for consumers’ health information and to level the competitive playing field among companies holding that information.⁸⁰

The Commission is not, however, proposing to make those changes at this time, because the commentary to the current Rule already provides guidance on the types of disclosures that the Commission considers to be “unauthorized.”⁸¹ Further, recent Commission orders, such as GoodRx, 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.”

Finally, Commission settlements establish important guidelines involving authorization.

⁷⁹ Lisa McKeen at 1 (recommending that the Rule require “express written acknowledgement and consent of the consumer/person(s) to which this information is personally owned”); Kaiser Permanente at 3 (“[T]he HBN Rule should require all [covered] entities to establish and follow notices of privacy and security practices [and] inform consumers about those notices in a prominent manner[.]”); AMA at 4-5 (identifying problems with consent structure and urging the Commission to presume “unauthorized access” “when an entity fails to disclose to an individual the specific secondary recipients of the individual’s data.”); AMIA at 2 (urging the Commission to presume that unauthorized access has occurred where an entity “fails to adequately disclose to individuals how user data is accessed, processed, used, reused, and disclosed.”).

⁸⁰ *E.g.*, OAG-CA at 5.

⁸¹ *See supra* note 49.

For example, the Commission’s recent settlement with GoodRx, alleging violations of the Rule, highlights that disclosures of PHR identifiable information inconsistent with a company’s privacy promises constitute an unauthorized disclosure.

The Commission seeks public comment about whether the commentary above and FTC enforcement actions 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.

To the extent that including such definitions would be appropriate, the Commission seeks comment on 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. The Commission also seeks comment on what constitutes acceptable methods of authorization, particularly when unauthorized sharing is occurring. For example, the Commission seeks 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?

Relatedly, the Commission seeks comment on 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. Finally, the Commission emphasizes that its decision to not define “authorization” or “affirmative express consent” does not mean that a “breach of security” is limited only to cybersecurity events.

2. Modifying Definition of Third Party Service Provider

The Commission also considered modifying the definition of “third party service provider.” Under the Rule, a “third party service provider” means an entity that “(1) [p]rovides 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) [a]ccesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services.⁸²” The 2009 Notice of Proposed Rulemaking notes that third party service providers include, for example, entities that provide billing or data storage services to vendors of personal health records or PHR related entities.⁸³ Although the Commission is not proposing to modify the definition of “third party service provider” at this time, the Commission requests comment on certain issues related to the definition. Given technological changes and the proliferation of new business models that have occurred since the Rule’s issuance, the Commission invites comments on the scope of entities that should be considered third party service providers under the Rule. While the 2009 Notice of Proposed Rulemaking

⁸² 16 CFR 318.2(h).

⁸³ 74 FR 17917 (Apr. 17, 2009) (“2009 Notice of Proposed Rulemaking”).

provides examples of third party service providers, the examples are illustrative. For example, under the Rule, should all advertising and analytics providers and platforms be considered third party service providers anytime they access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHR identifiable health information when providing services to vendors of personal health records and PHR related entities? Relatedly, the Commission requests comment on what it means to “provide services” under the Rule’s definition.

3. Changing Timing Requirements

The Commission also weighed whether to propose changing the Rule’s timing requirements. Specifically, the Commission considered public comments about whether the timing requirements were appropriate,⁸⁴ introduced unnecessary delay,⁸⁵ or did not give notifying entities sufficient time to investigate the facts of a breach.⁸⁶ One commenter expressed concern that the timing requirements do not provide consumers with important information as soon as would be valuable to them and there is no compelling reason for delaying notice.⁸⁷ Other commenters, however, expressed concern that entities experiencing a breach may not have sufficient information to be able to give the Commission a meaningful notification within 10 days.⁸⁸ These commenters recommended that the Commission extend the 10-day requirement for the notice to the FTC, consistent with the HIPAA Health Breach Notification Rule, which requires notification to the Secretary of HHS without unreasonable delay and in no case later than

⁸⁴ Lisa McKeen at 5; CHIME at 3; WEDI at 2.

⁸⁵ Hilal Johnson at 1.

⁸⁶ CARIN All. at 2; Allscripts at 2; Kaiser at 10.

⁸⁷ Hilal Johnson at 1.

⁸⁸ CARIN All. at 2; Allscripts at 2; Kaiser at 10.

60 calendar days following a breach.⁸⁹ Commission staff also consulted staff at HHS about its experience enforcing the HIPAA Health Breach Notification Rule regarding the timing requirements in that rule.

Although the Commission has not proposed any timing changes, the Commission requests comments on several issues related to timing. First, the Commission requests comment about the timing of notifications to consumers. In particular, the Commission requests comment regarding whether earlier notification of consumers would better protect them or whether it would lead to partial notifications, because the entity experiencing the breach may not have had time to identify all the relevant facts. Second, the Commission also requests additional comment on the timing of the notification to the FTC: 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.

IV. Paperwork Reduction Act

The Commission is submitting this Notice of Proposed Rulemaking and a Supporting Statement to the Office of Management and Budget (“OMB”) for review under the Paperwork Reduction Act (“PRA”) (44 U.S.C. 3501–3521). The breach notification requirements discussed above constitute “collections of information” for purposes of the PRA. *See* 5 CFR 1320.3(c). OMB has approved the Rule’s existing

⁸⁹ 45 CFR 164.408 (referencing timing requirement in 404).

information collection requirements through July 31, 2025 (OMB Control No. 3084-0150).

The proposed amendments to 16 CFR part 318 would likely result in more reportable breaches by covered entities to the FTC. In the event of a breach of security, the proposed Rule would require covered firms to investigate and, if certain conditions are met, notify consumers and the Commission.⁹⁰

Accordingly, staff has estimated the burdens associated with these proposed information collection requirements as set forth below.

Based on industry reports, staff estimates that the Commission's proposed information collection requirements will cover approximately 170,000 entities, which, in the event that they experience a breach, may be required to notify consumers and the Commission. While there are approximately 1.8 million apps in the Apple App Store⁹¹ and 2.7 million apps in the Google Play Store,⁹² as of November 2022 it appears that roughly 170,000 of the apps offered in either store are categorized as "Health and Fitness."⁹³ This figure for apps is a rough proxy for all covered PHRs, because most websites and connected health devices that would be subject to the Rule act in conjunction with an app.

⁹⁰ Third party service providers who experience a breach are required to notify the vendor of personal health records or PHR related entity, and then this firm would be required to notify consumers. The Commission expects that the cost of notification to third party service providers would be small, relative to the entities who have to notify consumers. The Commission invites comment on this issue and data that may be used to quantify the costs to third party service providers.

⁹¹ See App Store – Apple, <https://www.apple.com/app-store/> and App Store Data (2023) – Business of Apps, <https://www.businessofapps.com/data/app-stores/>.

⁹² App Store Data (2023) – Business of Apps, <https://www.businessofapps.com/data/app-stores/>.

⁹³ See App Store Data (2023), *supra* note 91, which reports 78,764 apps in the Apple App Store and 91,743 apps in the Google Play Store were categorized as "Health and Fitness" apps as of November 2022. This figure is likely both under- and over-inclusive. For example, this figure does not include apps categorized elsewhere (i.e., outside "Health and Fitness") that may be PHRs. However, at the same time, this figure also overestimates the number of covered entities, since many developers make more than one app.

Staff estimates that these entities will, cumulatively, experience 71 breaches per year for which notification may be required. With the proviso that there is insufficient data at this time about the number and incidence rate of breaches at entities covered by the Commission’s Rule (due to underreporting prior to issuance of the Policy Statement), 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 proposed Rule.⁹⁴ Additionally, as the number of breaches per year grew significantly in the recent years,⁹⁵ and staff expects this trend to continue, staff relied on the average number of breaches in 2021 and 2022 to estimate the annual breach incidence rate for HIPAA-covered entities.

Specifically, the HHS Office for Civil Rights (“OCR”) reported 715 breaches in 2021 and 717 breaches in 2022,⁹⁶ which results in an average of 716 of breaches for 2021 and 2022. Based on the 1.7 million entities that are covered by the HIPAA Breach Notification Rule⁹⁷ and the average number of breaches for 2021 and 2022, staff

⁹⁴ 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.

⁹⁵ According to the HHS Office for Civil Rights (“OCR”), the number of breaches per year grew from 358 in 2017 to 715 breaches in 2021 and 717 breaches in 2022. *See Breach Portal*, U.S. Dep’t of Health & Human Servs., Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (visited on March 2, 2023). The data was downloaded on March 2, 2023, resulting in limited data for 2023. Thus, breaches from 2023 were not considered. However, breach investigations that remain open (under investigation) are included in the count of yearly breaches.

⁹⁶ *See Breach Portal*, U.S. Dep’t of Health & Human Servs., Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (visited on March 2, 2023).

⁹⁷ In a recent Federal Register Notice (“FRN”) on Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, OCR proposes increasing the number of covered entities from 700,000 to 774,331. 86 FR 6446, 6497 (Jan. 21, 2021). The FRN also lists the number of covered Business Associates as 1,000,000 (Table 2).

determined an annual breach incidence rate of 0.00042 (716 / 1.7 million). Accordingly, multiplying the breach incidence rate (0.00042) by the estimated number of entities covered by the proposed information collection requirements (170,000) results in an estimated 71 breaches per year.

Costs

To determine the costs for purposes of this analysis, 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: 10,650

Estimated Annual Labor Cost: \$720,579

First, to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission, staff estimates that covered firms will require per breach, on average, 150 hours of employee labor at a cost of \$10,149.⁹⁸ This estimate does not include the cost of equipment or other tangible assets of the breached firms because they likely will use the equipment and other assets they have for ordinary business purposes. Based on the estimate that there will be 71 breaches per year the annual hours of burden for affected entities will be 10,650 hours (150 hours x 71 breaches) with an associated labor cost of \$720,579 (71 breaches × \$10,149).

⁹⁸ This estimate is the sum of 40 hours of marketing managerial time (at an average wage of \$73.77), 40 hours of computer programmer time (\$46.46), 20 hours of legal staff (\$71.17), 50 hours of computer and information systems managerial time (\$78.33). See Occupational Employment and Wage Statistics, U.S. Bureau of Labor Statistics (May 2021), https://www.bls.gov/oes/current/oes_nat.htm#00-0000.

Estimated Capital and Other Non-Labor Costs: \$49,463,046

The capital and non-labor costs associated with breach notifications depends upon the number of consumers contacted and whether covered firms are likely to retain the services of a forensic expert. For breaches affecting large numbers of consumers, covered firms are likely to retain the services of a forensic expert. FTC staff estimates that, for each breach requiring the services of forensic experts, forensic experts may spend approximately 40 hours to assist in the response to the cybersecurity intrusion, at an estimated cost of \$20,000.⁹⁹ FTC staff estimates that the services of forensic experts will be required in 60% of the 71 breaches. Based on the estimate that there will be 43 breaches per year requiring forensic experts (60% × 71 breaches), the annual hours burden for affected entities will be 1,720 hours (43 breaches requiring forensic experts × 40 hours) with an associated cost of \$860,000 (43 breaches requiring forensic experts × \$20,000).

Using the data on HIPAA-covered breach notices available from HHS for the years 2021-2022, FTC staff estimates that the average number of individuals affected per breach is 62,402.¹⁰⁰ Given an estimated 71 breaches per year, FTC staff estimates an average of 4,430,542 consumers per year will receive a breach notification (71 breaches × 62,402 individuals per breach).

⁹⁹ 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).

¹⁰⁰ HHS Breach Data, *supra* note 96 (mean of Individuals Affected during breaches 2017-2022). This analysis uses the last six years of HHS breach data to generate the average, in order to account for the variation in number of individuals affected by breaches observed in the HHS data over time.

Based on a recent study of data breach costs, staff estimates the cost of providing notice to consumers to be \$10.97 per breached record.¹⁰¹ This estimate includes the costs of electronic notice, letters, outbound calls or general notice to data subjects; and engagement of outside experts.¹⁰² Applied to the above-stated estimate of 4,430,542 consumers per year receiving breach notification yields an estimated total annual cost for all forms of notice to consumers of \$48,603,046 (4,430,542 consumers × \$10.97 per record). The estimated capital and non-labor costs total \$49,463,046 (\$860,000 + \$48,603,046).

Staff notes that these estimates likely overstate the costs imposed by the proposed Rule because: (1) it assumes that all entities covered by the Rule will be required to take all the steps required above; and (2) staff made conservative assumptions in developing many of the underlying estimates. Moreover, many entities covered by the Rule already have similar notification obligations under state data breach laws.¹⁰³ In addition, the Commission has taken several steps designed to limit the potential burden on covered

¹⁰¹ See IBM Security, Costs of a Data Breach Report 2022 (2022), <https://www.ibm.com/reports/data-breach> (“2022 IBM Security Report”). The research for the 2022 IBM Security Report is conducted independently by the Ponemon Institute, and the results are reported and published by IBM Security. Figure 2 of the 2022 IBM Security Report shows that cost per record of a breach was \$164 per record in 2022 and \$161 in 2021, resulting in an average cost of \$162.50. Figure 5 of the 2022 IBM Security Report shows that 7.1% (\$0.31m / \$4.35m) of the average cost of a data breach are due to “Notification” costs. The fraction of average breach costs due to “Notification” were 6.4% the previous year (IBM Security, Costs of a Data Breach Report 2021). Using the average of these numbers, staff estimates that notification costs per record across the two years are $6.75\% \times \$162.50 = \10.97 per record.

¹⁰² See 2022 IBM Security Report at 54.

¹⁰³ 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.

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 proposing expanded use of electronic notifications.

The Commission invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the FTC, including whether the information will have practical utility; (2) the accuracy of the FTC's estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of collecting information on those who respond.

Written comments and recommendations for the proposed information collection should also be sent within 30 days of publication of this document to <https://www.reginfo.gov/public/do/PRAMain>. Find this particular information collection by selecting "Currently under Review—Open for Public Comments" or by using the search function. The *reginfo.gov* web link is a United States Government website produced by OMB and the General Services Administration ("GSA"). Under PRA requirements, OMB's Office of Information and Regulatory Affairs ("OIRA") reviews Federal information collections.

V. Regulatory Flexibility Act

The Regulatory Flexibility Act ("RFA"), 5 U.S.C. 601 *et seq.*, requires that the Commission conduct an analysis of the anticipated economic impact of the proposed amendment on small entities. The purpose of a regulatory flexibility analysis is to ensure that an agency considers potential impacts on small entities and examines regulatory alternatives that could achieve the regulatory purpose while minimizing burdens on small

entities. The RFA 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, if any, unless the Commission certifies that the proposed rule will not have a significant economic impact on a substantial number of small entities. 5 U.S.C. 605.

The Commission believes that the proposed amendment would not have a significant economic impact upon small entities, although it may affect a substantial number of small businesses. Among other things, the proposed 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 proposed amendments improve the Rule’s readability by clarifying cross-references and adding statutory citations. The Commission does not anticipate these changes will add significant additional costs to entities covered by the Rule and the revisions to allow additional use of electronic notice may reduce costs for many entities covered by the Rule. Therefore, based on available information, the Commission certifies that amending the Rule as proposed will not have a significant economic impact on a substantial number of small entities. Although the Commission certifies under the RFA that the proposed amendment would not, if promulgated, have a significant impact on a substantial number of small entities, the Commission has determined, nonetheless, that it is appropriate to publish an IRFA to inquire into the impact of the proposed amendment on small entities. Therefore, the Commission has prepared the following analysis:

1. Description of the Reasons That Action by the Agency Is Being Considered

The Commission conducts a review of each of its rules ten years after issuance. In May 2020, the Commission requested public comment on whether technological and business changes warranted any changes to the Rule. After careful review of the comments received, the Commission concludes that there is a need to update certain Rule provisions. Therefore, it proposes modifications to the Rule as described in sections I and II.

2. Statement of the Objectives of, and Legal Basis for, the Proposed Rule

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

3. Description and Estimate of the Number of Small Entities to Which the Proposed Rule Will Apply

The proposed 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 proposed Rule will apply to approximately 170,000 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.¹⁰⁴ The Commission invites comment and information on this issue.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The Recovery Act and the proposed Rule impose certain reporting requirements within the meaning of the PRA. The proposed Rule will clarify which entities are subject to those reporting requirements. The Commission is seeking clearance from OMB for these requirements. Specifically, the Act and proposed Rule 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 proposed Rule 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 Act and proposed Rule 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 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 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

¹⁰⁴ 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>. The U.S. Small Business Administration (“SBA”) categorizes Software Publishers as a small business if the annual receipts are less than \$41.5 million.

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. The Commission seeks further comment on the costs and burdens of small entities in complying with the requirements of the proposed Rule.

5. *Other Duplicative, Overlapping, or Conflicting Federal Rules*

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would conflict with the proposed Rule. The HIPAA Breach Notification Rule applies to HIPAA-covered entities; the proposed Rule does not. The Commission invites comment and information about any potentially duplicative, overlapping, or conflicting federal statutes, rules, or policies.

6. *Description of any Significant Alternatives to the Proposed Rule*

In drafting the proposed Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the proposed changes to facilitate electronic notice will assist small entities by significantly reducing the costs of sending breach notices. In addition, the Commission is also proposing 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 potential 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 proposed Rule on small entities, while also comporting with the Recovery Act. The statutory requirements are specific as to the timing, method, and content of notice. Accordingly, the Commission seeks comment and information on ways

in which the Rule could be modified to reduce any costs or burdens for small entities consistent with the Recovery Act's mandated requirements.

VI. Instructions for Submitting Comments

You can file a comment online or on paper. For the Commission to consider your comment, we must receive it on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. Write "Health Breach Notification Rule, Project No. P205405" on the comment. Your comment—including your name and your state—will be placed on the public record of this proceeding, including the <https://www.regulations.gov> website.

Because of the agency's heightened security screening, postal mail addressed to the Commission is subject to delay. We strongly encourage you to submit your comments online through the <https://www.regulations.gov> website. To make sure the Commission considers your online comment, please follow the instructions on the web-based form.

If you file your comment on paper, write "Health Breach Notification Rule, Project No. P205405" on your comment and on the envelope, and mail your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue NW, Suite CC-5610 (Annex H), Washington, DC 20580.

Because your comment will be placed on the publicly accessible website at <https://www.regulations.gov>, you are solely responsible for making sure that your comment does not include any sensitive or confidential information. In particular, your comment should not include any sensitive personal information, such as your or anyone else's Social Security number; date of birth; driver's license number or other state identification number, or foreign country equivalent; passport number; financial account

number; or credit or debit card number. You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, your comment should not include any “trade secret or any commercial or financial information which . . . is privileged or confidential” – as provided by section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2) – including in particular competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

Comments containing material for which confidential treatment is requested must be filed in paper form, must be clearly labeled “Confidential,” and must comply with FTC Rule 4.9(c). In particular, the written request for confidential treatment that accompanies the comment must include the factual and legal basis for the request and must identify the specific portions of the comment to be withheld from the public record. Your comment will be kept confidential only if the FTC’s General Counsel grants your request in accordance with the law and the public interest. Once your comment has been posted publicly at www.regulations.gov, we cannot redact or remove your comment unless you submit a confidentiality request that meets the requirements for such treatment under FTC Rule 4.9(c), and the FTC’s General Counsel grants that request.

Visit the FTC website to read this document and the news release describing it. The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN *THE FEDERAL*

REGISTER]. For information on the Commission’s privacy policy, including routine uses permitted by the Privacy Act, see <https://www.ftc.gov/site-information/privacy-policy>.

List of Subjects in 16 CFR Part 318

Breach, Consumer protection, Health, Privacy, Reporting and recordkeeping requirements, Trade practices.

For the reasons set forth in the preamble, the Commission proposes to revise 16 CFR part 318 to read 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: Public Law 111-5, 123 Stat. 115 (2009).

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 web sites 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 web site 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* includes 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) *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:

(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 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:

(i) 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)).

(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 (Notice to FTC), 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 paragraphs (b) (Timing of notice to FTC) and (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 as soon as possible and in no case later than ten business days following the date of discovery of the breach. 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. Exemplar notices that vendors of personal health records or PHR related entities may use to notify individuals pursuant to this paragraph are attached as Appendix A.

(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 whether or not the individual's unsecured PHR identifiable health information may be 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; the potential harm that may result from the breach, such as medical or other identity theft; and 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, 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.

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

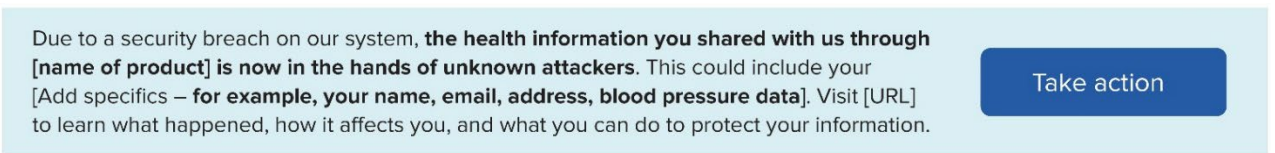
You shared health information with us when you used [product name]. **We discovered that we shared your health information with third parties for [if known, describe why the company shared the info] without your permission.** This could include your [Add specifics – **for example, your name, email, address, 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:



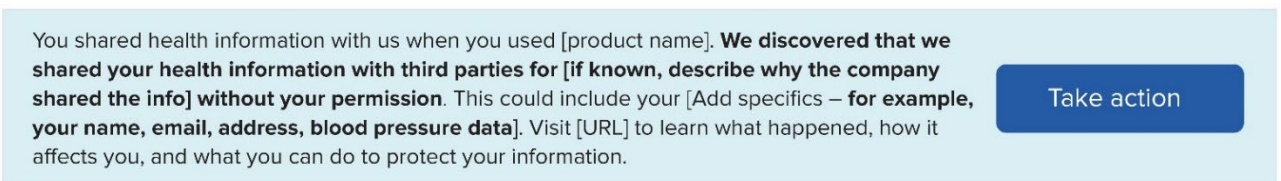
Due to a security breach on our system, **the health information you shared with us through [name of product] is now in the hands of unknown attackers.** This could include your [Add specifics – **for example, your name, email, address, blood pressure data**]. Visit [URL] to learn what happened, how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

Take action

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:



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.

Take action

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, 2022], we learned that an attacker had accessed a file containing our customers' health information on [February 28, 2022]. The file included your name, the name of your health insurance company, your date of birth, and your group or policy number.

A hacker could use your information now or at a later time to commit identity theft or could sell your information to other criminals. For example, a criminal could get medical care in your name or change your medical records or run up bills in your name.

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 to another company without your approval.

What happened?

We told Company XYZ (insert website address of Company XYZ) that you use our app, and between [January 10, 2021] and [March 1, 2022], we gave them your name and your email address.

We gave Company XYZ this information so they could use it for advertising and marketing purposes. For example, to target you for ads for cancer drugs.

You may contact Company XYZ at [insert contact info, such as email or phone] for more information.

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, 2022], we discovered that our employee had accidentally posted a database online on [February 28, 2022]. 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]