FUTURE OF PRIVACY FORUM

1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

August 8th, 2023

Via Electronic Mail

The Federal Trade Commission
Attention: Commission-2023-0037-0001
600 Pennsylvania Ave. N.W.
Washington, D.C. 20580

Re: Comments on NPRM - Clarifying the applicability of the Health Breach Notification Rule (HBNR) to apps and technologies (Commission-2023-0037-0001)

Dear Commissioners,

On behalf of the Future of Privacy Forum (FPF), we are pleased to provide comments and recommendations to the U.S. Federal Trade Commission regarding the Notice of Proposed Rulemaking (NPRM) on the applicability of the Health Breach Notification Rule (HBNR) to apps and technologies.[1] The NPRM presents an opportunity to enhance the protections afforded to sensitive and identifying health information as well as align the HBNR's language and definitions with the standards set by other regulatory definitions, such as the European Union's (EU) General Data Protection Regulation (GDPR).

FPF is a non-profit organization focused on advancing responsible data practices and fostering a privacy-conscious environment in the digital era.[2] As an institution dedicated to privacy and data protection, we have developed significant expertise in this space. We know that privacy is foundational to trust in patient-provider interactions and ongoing care, and even more so in evolving digital spaces and technologies.[3]

Introduction

The Federal Trade Commission (hereafter "the Commission") has made the protection of health data privacy a priority, particularly where health data falls outside the protection of sectoral

[1] 88 Fed. Reg. 37819 (June 9, 2023), https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule.
[2] The views expressed in this comment are those of FPF and do not necessarily represent the opinions of our supporters or Advisory Board.
[3] Billie Murray and Susan McCrone, *An integrative review of promoting trust in the patient-primary care provider relationship*, 71 J. Adv. Nurs. 3 (2015), https://pubmed.ncbi.nlm.nih.gov/25113235/; Paige Nong, et al., *Discrimination, trust, and withholding information from providers: Implications for missing data and inequity*, 18 SSM Popul. Health 101092 (2022), https://pubmed.ncbi.nlm.nih.gov/35479582/; Matthew Ridd et al., *The patient–doctor relationship: a synthesis of the qualitative literature on patients' perspectives*, 59 Br. J. Gen. Pract. e116 (2009), https://pubmed.ncbi.nlm.nih.gov/19341547/.

regulations such as the Health Information Portability and Accountability Act (HIPAA) and the jurisdiction of the U.S. Department of Health and Human Services (HHS). In this Comment, FPF focuses our recommendations on the Commission's proposed amendments to the scope of the HBNR and the "breach of security" definition.[4]

Specifically, FPF offers the following recommendations:

Section 1: Recommendations Regarding Amendments Aimed at Clarifying the Rule's Scope

A. Define a Standard for Identifiability for "PHR identifiable health data" to Clearly Expand Protections for a Broad Spectrum of Personal Information
B. Define "Relates to" to Include the Creation of Health-Related Inferences from a Wide Range of Routine Commercial Datasets, While Establishing Clear Obligations for Businesses

Section 2: Recommendations Regarding Amendments to the Definition of "Breach of Security"

C. Establish Clear Guidelines for Intentional Data Sharing that Does Not Require Affirmative Consent
D. Ensure that the Rule Contains "Good Faith" Exceptions for Merely Technical Violations
E. Further Define "Breach of Security" to Clarify Where the Commission May Take Enforcement Action.

SECTION 1: RECOMMENDATIONS REGARDING AMENDMENTS AIMED AT CLARIFYING THE RULE'S SCOPE

One of the Commission's stated goals for the proposed rules is to clarify the scope of the HBNR and the technologies and entities it covers. In this section, we provide two recommendations to help the Commission accomplish this goal, suggesting that the Commission establish: 1) a standard of identifiability to aid the categorization of identifiable versus de-identified information, and 2) additional guidance for inferences that relate to an individual's health created from data that is not health data on its face.

[4] *Supra* note 1, at 3, According to the NPRM, the Commission seeks to amend the Rule to "(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."

A. Define a Standard for Identifiability for "PHR identifiable health information" to Clearly Expand Protections for a Broad Spectrum of Personal Information

The proposed Rule would modify and add a third prong to the definition of "PHR identifiable health information" while otherwise not altering the other two prongs.[5] This addition will help provide clarity to the Rule. However, FPF recommends that the Commission revisit the rest of the definition. Specifically, the Commission should include a standard for reasonable identifiability for when information constitutes "PHR identifiable health information" to best allow the Commission in its enforcement of the Rule to keep pace with rapidly evolving technology and help covered entities to streamline their compliance with leading data protection laws, protect sensitive health information, respond effectively to data breaches, and foster public trust in their data handling practices.

The current definition of "PHR identifiable health information" is "individually identifiable health information," and, with respect to an individual, information "that is provided by or on behalf of the individual" and "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."[6] In contrast, leading global and U.S. standards define "personal information" and incorporate standards of reasonable identifiability that do not rest on an organization's beliefs or knowledge. For example, the GDPR broadly governs "any information concerning an identified or *identifiable* natural person"[7] (emphasis added), while the Colorado Privacy Act defines personal data to include "information that is linked or *reasonably linkable* to an identified or identifiable individual."[8] (emphasis added)

An approach based on reasonable linkability, rather than based on an organization's belief or knowledge, would be better suited to protect a wide range of personal information that is linkable to an individual, even if that individual is not "identified" in the sense of their name being known. This can include certain information like device identifiers that are linked to smartphones, browsers, or wearable health devices. It can also include "indirect identifiers," or information that can be used to re-identify individuals when combined with external information: information such as dates and places of medical appointments, demographic information (race, ethnicity), or socioeconomic variables (occupation, salary). This may also include unique health diagnoses or rare health conditions, which are increasingly identifiable in small populations.[9] When such identifiers are widely shared or sold without controls, the risk of identification is clear.

---

[5] *Supra* note 1.
[6] *Id.*
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter the General Data Protection Regulation or GDPR) (Text with EEA relevance), 119 OJ L (2016), http://data.europa.eu/eli/reg/2016/679/oj/eng (last visited Aug. 3, 2023).
[8] The Colorado Privacy Act (CPA), Colo. Rev. Stat. § 6-1-1301 et seq.
[9] *See Havasupai Tribe v. Arizona Board of Regents*, *infra* note 31, at 1081.

This approach is also more consistent with the Commission's other guidance on data identifiability.[10] For instance, the current guidance for general consumer data provides a three-part definition of de-identified data (and by extension, of identifiability).[11] This definition, which has been adopted by many state-level comprehensive and health-specific privacy laws,[12] states that "[d]ata is not 'reasonably linkable' [to an individual] to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[13]

Clear standards of identifiability are crucial controls for health data, particularly data that may be used by bad actors to harm individuals or small populations. Defined standards of identifiability will aid covered entities in categorizing identifiable health information and provide guardrails for its handling throughout the consumer data ecosystem. The first step to this is recognizing that the identifiability of data exists on a spectrum rather than as a binary and depends on a wide range of factors, including the specific context.[14]

In the context of the current text of the HBNR, as modified by the proposed rulemaking (below, *italics*), a more protective standard of identifiability may appear as follows (***bold italics***):

> PHR identifiable health information includes information,
>
> a. that is provided by or on behalf of the individual; and
>
> *b.* ~~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.~~ ***that is reasonably related to an identified or identifiable natural person.*** *It does not*

[10] "Protecting Consumer Privacy In An Era of Rapid Change," The Federal Trade Commission (Mar. 2012) at 21, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[11] *See, id.*; *see also* "[D]e-identification is a process that is applied to a dataset with the goal of preventing or limiting informational risks to individuals, protected groups, and establishments while still allowing for meaningful statistical analysis." Simson Garfinkel et al., *De-Identifying Government Data Sets*, National Institution of Standards and Technology, (Nov. 15, 2022), https://csrc.nist.gov/publications/detail/sp/800-188/draft. As two sides of the same coin, a clear standard of identifiability assists in supporting a standard of de-identification.

[12] *See, ex.* The Connecticut Data Privacy Act (CDPA), Public Act No. 22-15; The Colorado Privacy Act (CPA) Colo. Rev. Stat. § 6-1-1301 *et seq.*; The "My Health, My Data" Act (MHMD), Washington House Bill 1155 (2023).

[13] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers,* (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[14] *In re BetterHelp, Inc.*, No. 2023169 (Mar. 2, 2023).

include data that has been de-identified 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;

c. *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*
d. *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)).*[15]

B. Define "Relates to" to Include the Creation of Health-Related Inferences from a Wide Range of Routine Commercial Datasets, While Establishing Clear Obligations for Businesses

The proposed Rule would expand the definition of "PHR identifiable health information" to include information that "*relates to* the past, present, or future physical or mental health 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" (emphasis added).[16] In order to ensure operationalizable clarity in the scope of this definition, the Commission should establish guidance for when the results of inferences about an individual's health constitute "PHR identifiable health information."[17] Health information may be formally or informally inferred based on queries and analysis of data that would not be considered health data standing alone.[18]

Although the HBNR's proposed definition of "PHR identifiable health information" is in line with emerging health data protection laws, without additional clarity it poses a significant challenge for

[15] In broadening the definition of "identifiable" health information, the Commission would be in line with previous rulemaking efforts that have allowed the Commission to keep up with changing technology and business practices. For example, in the 2013 rulemaking, the Commission expanded the definition of "personal information" under the Children's Online Privacy Protection Act (COPPA) in order to accommodate the rise in smartphone apps and associated sharing of device identifiers and precise geolocation. Similarly, the Commission should now update its standards under the HBNR to reflect rapid changes in the last 14 years.
[16] *Supra* note 1.
[17] *Id*.
[18] *See, ex.,* infra at 21.

covered entities.[19] This is because almost all personal information holds the potential to reveal information about a person's health. For example, researchers have demonstrated that car ownership can be predictive of general health status and that they can accurately infer a person's levels of tobacco, drug, and alcohol use from their social media posts, depression from smartphone usage data, and health condition and diagnosis information from search data.[20] At the same time, businesses have many valid non-health related purposes for processing this same data: car ownership data may be used to advance or analyze transportation equity, social media posts may be studied to track disinformation, and smartphone usage and search data may be processed to offer non-health services or make product improvements.[21]

The HBNR should distinguish health data as a category deserving heightened protections while permitting covered entities to maintain a clear ability to process data that is facially not related to health, for non-health purposes. When an organization makes inferential conclusions about health, the access or use of the results may raise many of the same risks as the access or use of

[19] Health data privacy laws recently passed in Washington State and Nevada both create protections for, "information…that is derived or extrapolated from information that is not consumer health data, including, without limitation, proxy, derivative, inferred or emergent data derived through an algorithm, machine learning or any other means." Likewise, state-level comprehensive privacy laws may also create protections for health inferences. The Colorado Privacy Act defines "sensitive data" as including "personal data revealing . . . a mental or physical health condition or diagnosis." The implementing rules for the CPA note that, "'[r]evealing,' as referred to in…[the CPA's definition of "sensitive data"] includes [s]ensitive [d]ata Inferences. For example…precise geolocation data which is used to infer an individual visited a reproductive health clinic and is used to infer an individual's health condition…is considered [s]ensitive [d]ata under [the CPA]."

[20] *See, ex.* Roy Carr-Hill and Paul Chalmers-Dixon, "The Public Health Observatory Handbook of Health Inequalities Measurement," South East England Public Health Observatory (2005), at 101 (observing that there is a demonstrable "relation between lack of car ownership and poor health."); Mason Marks, "Emergent Medical Data," Harvard Law School's 'Bill of Health' Blog (Oct. 11, 2017), https://blog.petrieflom.law.harvard.edu/2017/10/11/emergent-medical-data/; Fabian Wahle, Tobias Kowatsch, Elgar Fleisch, Michael Rufer, and Steffi Weidt, *Mobile Sensing and Support for People With Depression: A Pilot Trial in the Wild*, 4 JMIR Health 3 (2016), https://mhealth.jmir.org/2016/3/e111/; Sidney Fussell, "Google's Totally Creepy, Totally Legal Health-Data Harvesting," The Atlantic (Nov. 14, 2019), https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999/.

[21] *See, ex.,* Jedd Davis, Dave Nussbaum, and Kevin Troyanos, "Approach Your Data with a Product Mindset," Harvard Business Review (May 12, 2020), https://hbr.org/2020/05/approach-your-data-with-a-product-mindset; "Car access: Everyone needs reliable transportation access and in most American communities that means a car," National Equity Atlas, https://nationalequityatlas.org/indicators/Car_access (last visited Aug. 7, 2023); Irene V. Pasquetto et al., "Tackling misinformation: What researchers could do with social media data," Harvard Kennedy School Misinformation Review (Dec. 9, 2020), https://misinforeview.hks.harvard.edu/article/tackling-misinformation-what-researchers-could-do-with-social-media-data/.

traditional health information (such as health conditions or diagnosis status). As such, it is critically important to establish appropriate protections for the results of health-related inferences.[22]

So far, companies have largely responded to current regulatory uncertainty by taking a risk-based approach to categorizing information, but specific practices vary widely.[23] There remains very little guidance available for navigating when information is, or is not, revealing of health.[24] As a result, the Commission has an important opportunity to codify its growing "case law" of enforcement decisions and provide clear, national guidance on the question of "inferences."[25] Guidance that establishes that information that may not be facially "health data" can nonetheless *become* PHR identifiable health data based on the context of its use or purpose would provide direction for regulated entities to assess whether their data processing falls into this category.[26]

We recommend that the Commission develop guidance that recognizes use- and purpose-based factors regarding the conditions under which the results of any inferences that a regulated entity makes about an individual's health constitute "PHR identifiable health information." Relevant factors should include the deliberate processing to reveal health information as well as the quality, or "closeness," of the health inference.

---

[22] *See, ex*. "The Data Will See You Now," The Ada Lovelace Institute (Oct. 2020), https://www.adalovelaceinstitute.org/wp-content/uploads/2020/11/The-data-will-see-you-now-Ada-Lovelace-Institute-Oct-2020.pdf (noting that, "[the] datafication [of healthcare] raises significant concerns… It makes individuals' health legible to a broad array of actors outside recognised medical and clinical settings, giving those with the appropriate digital tools an increased ability to know about, and engage with, people's health through their data. Datafication also creates increasingly comprehensive and quantified renderings of health, creating the conditions for disempowerment and providing unprecedented opportunities to monitor and influence people"); Charlie Warzel, "All Your Data is Health Data," The New York Times (Aug. 13, 2019), https://www.nytimes.com/2019/08/13/opinion/health-data.html (noting that health information can be inferred from an incredibly broad range of seemingly-innocuous data points).

[23] *See, ex*. Divya Sridhar, "Consumer health data: A risk-based approach to digital privacy," The International Association of Privacy Professionals (June 8, 2021), https://iapp.org/news/a/consumer-health-data-a-risk-based-approach-to-digital-privacy/.

[24] The guidance that does exist is fairly minimal. *See, ex.,* "Protecting Washingtonians' Personal Health Data and Privacy," Washington State Office of the Attorney General, https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

[25] *See FTC v. GoodRx Holdings, Inc.*, No. 2023090 (N.D. Cal. Feb. 1, 2023); *In re BetterHelp, Inc.*, No. 2023169 (Mar. 2, 2023).

[26] Elisa Jillson, "Protecting the privacy of health information: A baker's dozen takeaways from Commission cases," The Federal Trade Commission (Jul. 25, 2023), https://www.Commission.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-Commission-cases (noting that, "[h]ealth information isn't just about medications, procedures, and diagnoses. Rather, it's anything that conveys information – or enables an inference – about a consumer's health.").

- ***Deliberate Processing to Reveal Health Information:*** The manner in which an entity processes information will often determine whether it "relates to" a health condition.[27] For example, certain consumer purchase information, geolocation information indicative of certain lifestyle or food choices, or education status may become PHR identifiable information when processed to reveal something about an individual's health status. Conversely, other information, such as precise geolocation information that reveals that a particular individual (or set of individuals) visited an abortion or other health clinic, is likely *per se* health data.[28]

- ***The Closeness of the Inference:*** The quality, or closeness, or inference is also relevant to whether health inferences should be considered PHR identifiable information.[29] For example, the Commission has previously determined that in the context of a provider of mental health services, sharing of email addresses linked to the identity of the provider constituted "health information" because of a close inference that the contact information was provided by individuals seeking mental health services.[30]

As advanced processing techniques continue to increase the ability to more accurately infer health information from even seemingly unrelated, non-health information, our understanding of

---

[27] For example, guidance on the United Kingdom (UK) General Data Protection Regulation (GDPR) from the UK's Information Commission Office (ICO) (hereinafter "UK's ICO guidance") clarifies that "[b]iometric data is…special category data whenever you process it 'for the purpose of uniquely identifying a natural person.'" United Kingdom Information Commissioner's Office, "What is Special Category Data?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/ (last visited Jul. 23, 2023).

[28] *See* Charles Duhigg, "How Companies Learn Your Secrets," The New York Times (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Michael Rozier et al. "Personal Location as Health-Related Data: Public Knowledge, Public Concern, and Personal Action," Value in Health (May 24, 2023), https://www.sciencedirect.com/science/article/abs/pii/S109830152302614; *See* Education Access and Quality, U.S. Department of Health & Human Services, https://health.gov/healthypeople/objectives-and-data/browse-objectives/education-access-and-quality (noting that, "[p]eople with higher levels of education are more likely to be healthier and live longer."); Kristin Cohen, "Location, health, and other sensitive information: Commission committed to fully enforcing the law against illegal use and sharing of highly sensitive data," The Federal Trade Commission (Jul. 11, 2022), https://www.Commission.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-Commission-committed-fully-enforcing-law-against-illegal.

[29] As noted by the UK ICO, "whether or not an inference should be treated as sensitive data depends on how certain that inference is, and whether you are deliberately drawing that inference. If you can infer relevant information with a reasonable degree of certainty then it's likely to be special category data even if it's not a cast-iron certainty." United Kingdom Information Commissioner's Office, "What is Special Category Data?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-is-special-category-data/ (last visited Jul. 23, 2023).

[30] *Supra* note 14.

health data must also evolve to protect such inferences.[31] By specifying that health inferences can constitute PHR identifiable information, the Commission will establish strong protections for this category of information that are responsive to the contemporary modern data environment.

SECTION 2: RECOMMENDATIONS REGARDING AMENDMENTS TO THE DEFINITION OF "BREACH OF SECURITY"

A core goal of the Commission in the proposed Rules is to expand "breach of security" to include not only security failures but also instances of intentional sharing of data without or beyond the individual's permission or consent. Recent complaints filed by the Commission have asserted that breaches of security include unauthorized disclosures, transfers, and sharing of PHR identifiable information.[32] However, there is significant controversy about whether and to what extent privacy violations should constitute a "breach of security."[33] Therefore, if the Commission continues to follow this approach, it must provide operational clarity about the Commission's expectations and actions that may lead to enforcement action.[34]

In this section, we offer three recommendations to enhance understanding of the Rule: 1) establish clear guidelines for intentional data sharing that does not require affirmative consent, 2) outline good faith exceptions for certain unauthorized disclosures that present a low probability of risk and in which the information is not used for an unauthorized purpose or subject to further unauthorized disclosure, and 3) further define "breach of security" to clarify where the Commission may take enforcement action.

---

[31] "The Data Will See You Now," The Ada Lovelace Institute (Oct. 2020), https://www.adalovelaceinstitute.org/wp-content/uploads/2020/11/The-data-will-see-you-now-Ada-Lovelace-Institute-Oct-2020.pdf (noting that, "[t]he increasing datafication of health has not only expanded what counts as data related to health. It has also changed the contexts in which data about health is generated, gathered, stored and processed."

[32] *See, e.g. FTC v. GoodRx Holdings, Inc.*, No. 2023090 (N.D. Cal. Feb. 1, 2023); *United States v. Easy Healthcare Corporation,* No. 1:23-cv-3107 (N.D. Ill. May 17, 2023).

[33] *Compare*, HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 ("[a] breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information") *with* Brief for Electronic Frontier Foundation (EFF) as Amicus Curiae, *Van Buren v. United States*, at 4 (arguing that the Computer Fraud and Abuse Act (CFAA) was passed to target computer break-ins and should not turn into "an all purpose mechanism for policing objectionable or simply undesirable behavior").

[34] In a subset of cases, "exceeding authorized access" would be very similar to the question of "unauthorized access," or the sharing of information without an individual's permission. However, not all intentional sharing of data between businesses is conducted with consent (for example, sharing with service providers, as discussed below in Part IV). As a result, there is a benefit to clarifying that "exceeding authorized access" will constitute a breach in all cases.

C. Establish Clear Guidelines for Intentional Data Sharing that Does Not Require Affirmative Consent

Under an expanded interpretation of "breach," the proposed Rule would apply to situations involving the intentional sharing of data between covered entities and third parties or vendors, either without the individual's consent or in a manner that exceeds that consent. In many cases, affirmative consent is the appropriate requirement for sensitive health information. However, consent is not appropriate, helpful, or even possible in all situations of intentional data sharing, and in some cases may even cause harm. For example, an organization may share information with a service provider operating on their behalf to provide storage; may share information to protect the safety or vital interests of an individual or react to a public health emergency; or to protect themselves against security incidents and fraud. In each of these situations, data protection laws typically invoke a variety of non-consent measures, including data minimization, transparency, notice to the end-user or the regulator, and opportunities to object.

As a baseline, covered entities should not be required to obtain individual consent before sharing data with valid service providers, or entities that process data *solely* on their behalf. Service providers (or "processors" under the GDPR) must typically process data solely on behalf of the covered entity, and may not re-use, or further share or sell, the data for any incompatible secondary purposes. A common example is cloud storage providers: cloud storage is a common need for many PHR vendors, and does not typically require further secondary uses.

The Commission's definition of "third party service provider," if adopted for this purpose, may require additional revision to bring it in line with existing data protection norms. For example, a service provider should be prohibited from using data for secondary, incompatible uses beyond processing on behalf of the main entity. Furthermore, the Commission may choose to adopt similar affirmative requirements for service providers as seen in existing privacy laws, such as contractual obligations that promote responsible data stewardship and create liability for further sale, disclosure, or use of the information for secondary, incompatible purposes. Some emerging data protection laws also require service providers to obtain written authorization prior to engaging their own service providers, or subprocessors.

D. Ensure that the Rule Contains "Good Faith" Exceptions for Merely Technical Violations

Along with the rise in harmful security breaches in recent decades, there has also been a rise in the number of "unauthorized disclosures" that may be technical violations, but not create sufficiently significant privacy or security risks to warrant notification. As a result, the Commission

should provide similar good faith exceptions to those that are well-established in HIPAA and in state data breach notification laws.[35]

FPF recommends that the HBNR provide some variation of the following language that is typical of both HIPAA and state data breach notification laws:

> ***The good faith acquisition of unsecured PHR identifiable health information is not a breach of security. Good faith acquisition includes the following applications, provided that that information is not used for an unauthorized purpose or subject to further unauthorized disclosure:***
>
> 1. ***When an employee unintentionally acquires, accesses, or uses PHR identifiable health information within the scope of their authority;***
> 2. ***When a person authorized to access PHR identifiable information accidentally shares PHI with another authorized person at the same organization, and the information is not further disclosed in a manner not permitted by the Rule;***
> 3. ***The unauthorized person or entity receiving the information wouldn't have been able to retain it***

Including good faith exceptions would align with the HBNR's statutory goals of incentivizing economic growth in health information technologies while creating expanded privacy and security protections to counteract increased risk.[36] Broadly requiring covered entities to report every instance of unauthorized disclosure or disclosure that exceeds authorized access would not only not help achieve that end, nor be necessary to protect consumers, but it may have the opposite effect. Over-reporting data breaches can erode the confidence that customers, patients, members, partners, and others have covered entities' ability to protect their privacy, likely

[35] "Security Breach Notification Laws," National Conference of State Legislatures (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws (noting that "security breach laws typically have provisions regarding who must comply with the law," including exemptions such as encrypted information); "Data Breach Reporting Requirements," Federal Communications Commission Proposed Rule (Jan. 1, 2023), https://www.federalregister.gov/documents/2023/01/23/2023-00824/data-breach-reporting-requirements (noting that, "with only a few exceptions, the vast majority of state statutes include a provision exempting from the definition of breach a good-faith acquisition of covered data by an employee or agent of the company where such information is not used improperly or further disclosed"); The Health Information Portability and Accountability Act (HIPAA) Breach Notification Rule, 45 CFR §§ 164.400-414.

[36] The Health Information Technology for Economic and Clinical Health Act (HITECH Act), 42 U.S.C. §. 139w-4(0)(2) (Feb. 2009), enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (2009).

resulting in overall consumer distrust in health information technologies.[37] It may also generally lead to less internal transparency within covered entities for fear of retaliation.[38]

Take, for instance, the scenario provided in the 2009 NPRM regarding an employee that "inadvertently accessed the database, realized that it was not the one he or she intended to view, and logged off without reading, using, or disclosing anything."[39] Such a situation may constitute a breach under the current NPRM text, but it does not present the risk of harm that warrants notification to the individuals or government regulators as scenarios where the information is subsequently misused or subject to further disclosure by the employee. In fact, reporting such a situation may cause unnecessary strife to the individuals who are not at risk, and perhaps lead to notification fatigue or even an adverse employment action against the employee due to public or consumer backlash.[40]

E. Further Define "Breach of Security" to Clarify Where the Commission May Take Enforcement Action

The proposed Rule would amend "breach of security" to include both data security incidents and "unauthorized disclosures"–essentially codifying the Commission's interpretation in *GoodRx* and *Easy Healthcare* that disclosures to third parties without the individuals' consent are breaches of security under the HBNR.[41] However, the current language and context of the proposed Rule create significant complexity for organizations navigating the distinct privacy and security concepts at the heart of the HBNR. As such, in order to ensure that organizations are on notice of the full extent to which the Commission may take action as a violation of the Rule, FPF recommends that the Commission clarify the Rule to reflect whether it applies only to situations where disclosure is "unauthorized" or also to situations in which a use of data exceeds a recipient's or accessing party's authorized access.

---

[37] "ICO warns about over-reporting data breaches under GDPR," The International Association of Privacy Professionals (Sept. 14, 2018), https://iapp.org/news/a/ico-warns-about-over-reporting-data-breaches-under-gdpr/; "Over-reporting vs. under-reporting data breaches," Experian (Sept. 20, 2011), https://www.experian.com/blogs/data-breach/2011/09/20/over-reporting-vs-under-reporting-data-breaches/ ; "Too Much or Too Little? The Risks of Under- or Over-Reporting Data Breaches," RadarFirst, https://www.radarfirst.com/blog/too-much-or-too-little-the-risks-of-under-or-over-reporting-incidents/ (last visited Aug. 3, 2023).

[38] "A third of organizations admit to covering up data breaches," VentureBeat (Apr. 5, 2023), https://venturebeat.com/security/a-third-of-organizations-admit-to-covering-up-data-breaches/ (observing that employees may have incentives to under-report breaches to their employers).

[39] *Supra* note 1.

[40] "Understanding and Fighting Alert Fatigue," Atlassian, https://www.atlassian.com/incident-management/on-call/alert-fatigue (last visited Aug. 4, 2023).

[41] *FTC v. GoodRx Holdings, Inc.*, No. 2023090 (N.D. Cal. Feb. 1, 2023); *United States v. Easy Healthcare Corporation,* No. 1:23-cv-3107 (N.D. Ill. May 17, 2023).

While privacy and data security are inherently connected, laws regarding these topics are typically created and framed with distinct intents and scopes.[42] As a result, even a serious privacy violation may not always result in a violation of a security or breach notification law.[43] In *Van Buren v. United States*, the Supreme Court similarly analyzed whether "authorized access" within the Computer Fraud and Abuse Act (CFAA) was purpose-based, and should apply to a police officer who misused his law enforcement credentials to obtain and sell someone's license plate information.[44] The majority found the precise language in the CFAA does not cover those who have improper motives for obtaining information that is otherwise available to them, noting that a rule drafted to protect against only typical "hacking" scenarios is ill-fitted "to remediating 'misuse' of sensitive information."[45]

[42] A security breach typically involves unauthorized access, use, or disclosure of sensitive data due to a failure in the protective measures put in place. On the other hand, a privacy violation might involve the misuse of personal information that was legally collected, but the usage goes beyond the initial consent or legitimate purpose. *Compare* Michael Chargo, *You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data*, Tenn. J. Bus. L. 115 (2018-2019) (describing breaches of data security as the result of hacker activity); Seena Gressin, "The Equifax Data Breach: What to Do," The Federal Trade Commission (Sept. 8, 2017), https://www.penncommunitybank.com/wp-content/uploads/2019/12/The-Equifax-Data-Breach_-What-to-Do-_-Consumer-Information.pdf (discussing the 2017 Equifax data breach, which involved "hackers accessed people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people."); Nathan Manworren, Joshua Letwat, and Olivia Daily, "Why you should care about the Target data breach," 59 Business Horizons 3 (2016) (describing how the 2013 Target data breach was perpetuated by "someone [who] installed malicious software (malware) on Target's security and payments system)" *with* "FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology," Federal Trade Commission (May 7, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology (describing a photo app developer's deceptive use of user data in a way that exceeded user consent) *and* "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others," The Federal Trade Commission (June 22, 2021) (describing a femtech app's deceptive sharing of sensitive health data for marketing purposes despite having represented to users that their data would be kept private.

[43] As a result, security laws often fall short of offering the full range of necessary privacy safeguards to protect individual rights and freedoms. *See*, *e.g.*, Daniel Solove and Woodrow Hartzog, "Breached!: Why Data Security Law Fails and How to Improve it," Oxford University Press 2022 (stating that "front door hacking," or the use of permissible access mechanisms for unauthorized purposes, while not the same in practice, can still cause the same effects as "backdoor" cybersecurity incidents).

[44] *Van Buren v. United States*, 593 US _ (2021).

[45] *Id*. at 15.

Language that refers to "exceed[ing] authorized access" is different from "unauthorized disclosure."[46] For instance, it may include specific situations raised by the Commission where (1) the covered entity has received PHR identifiable information from an individual with affirmative consent but uses or discloses it for additional, incompatible purposes; as well as situations where (2) an acquiring entity obtains the PHR identifiable information through legitimate means for an impermissible purpose.

The Commission has focused attention on situations involving "exceeding authorized access" in other notable security breaches outside of the health context,[47] and in illustrations raised during the rulemaking process–but has not yet explicitly clarified the inclusion of these examples in the text of the HBNR. For instance, the Commission provides a hypothetical example in the 2009 Notice of Proposed Rulemaking for the HBNR, where an employee of a health system obtained access to PHR identifiable health information by using a database of personal health records maintained by his employer.[48] In one scenario, the employee viewed the records to find health information about a particular public figure and sold the information to a national gossip magazine, and in a second scenario, the employee viewed the records to obtain information about his or her friends. If the Commission's intent is for both scenarios to be treated as a security breach, the currently proposed text of the HBNR does not yet make it obvious that the acquisitions are within the scope of the Rule if the employee viewed health records using legitimate means.

In a similar vein, adopting a framework centered around "exceeding authorized access" may be better suited to the scenario emphasized by the Commission on pages 24-25 of the present NPRM. In this scenario, an individual grants authorization to a service provider for the collection of their personally identifiable health information, only for the service provider to subsequently sell this information to another entity without the individual's knowledge or consent. While the acquiring entity lacked the individual's explicit consent to access this data, it could be argued that

[46] In a subset of cases, "exceeding authorized access" would be very similar to the question of "unauthorized access," or the sharing of information without an individual's permission. However, not all intentional sharing of data between businesses is conducted with consent (for example, sharing with service providers, as discussed below in Part IV). As a result, there is a benefit to clarifying that "exceeding authorized access" will constitute a breach in all cases.
[47] For example, in a 2006 incident involving ChoicePoint, a provider of consumer reports, the company gave access to credit reports and social security numbers to a malicious actor who posed as a legitimate ChoicePoint customer and used their customer access to purchase the data for nefarious purposes. Despite the actors' use of legitimate channels, the Commission categorized the incident as a data breach and a violation of the Fair Credit Reporting Act (FCRA) due to the fact that the actor did not have a permissible purpose to obtain them. *United States v. ChoicePoint*, 1:06-cv-00198 (N.D. Ga. 2006).
[48] 74 Fed. Reg. 17915 (Apr. 20, 2009) https://www.federalregister.gov/documents/2009/04/20/E9-8882/health-breach-notification-rule.

the initial consent given by the individual for collection implies some degree of authorization. But, there is little ambiguity that the data sharing was beyond the scope of her initial consent.

In such scenarios, the corpus of data protection law offers a more robust set of tools that can be granted by security or breach notification laws alone, including broad safeguards for data minimization, retention, purpose specification, transparency, and individual rights to consent or object to uses of data. However, if the Commission aims to expand the scope of the HBNR from traditional security concepts to include core privacy and data protection safeguards, it should do so without ambiguity. Clear and enforceable guardrails on exceeding the scope of consent or authorization will allow covered entities to better understand their obligations.

Conclusion

Thank you for this opportunity to respond to the Commission's proposal. If you would like additional information or have questions on any of the information provided herein, you may contact Jordan Wrigley, Researcher for Health & Wellness at jwrigley@fpf.org.

Sincerely,
The Future of Privacy Forum

Jordan Wrigley, Researcher for Health & Wellness
Tatiana Rice, Senior Counsel
Felicity Slater, Policy Fellow
Stephanie Wong, Policy Fellow
Stacey Gray, Senior Director for U.S. Policy
Niharika Vattikonda, Health & Wellness Intern
Randy Cantz, Ethics & Data Sharing Intern