Changes to the Federal Trade Commission (FTC) Health Breach Notification Rule closes some gaps but adds some ambiguity

Received (in revised form): 2nd September, 2024

Trinity Car
Managing Counsel, Privacy, Syneos Health, USA

Trinity is the managing counsel for a Fortune 1000 company and a designated privacy law specialist with a strong industry focus on health care and life sciences. In addition to advising on data protection laws, Trinity also serves as the Canadian DPO and regularly provides guidance on GDPR compliance. She has a deep understanding of the applicability of the Health Insurance Portability and Accountability Act (HIPAA) to health care and research. Trinity has extensive experience advising clients ranging in size and maturity from newly public to Fortune 200 in a variety of areas including implementing emerging technologies, advising on complex data flows, negotiating large technology deals, incident response, M&A, privacy contracting (including legitimising international data transfer) and global privacy compliance. Trinity is a frequent speaker and author on privacy-related topics and holds a CIPP/US, CIPM and FIP in addition to her PLS from the IAPP.

Syneos Health, 1030 Sync Street, Morrisville, North Carolina, 27650, USA
Tel: +1 984 459 5377; E-mail: trinity.car@syneoshealth.com

Brad Rostolsky
Shareholder, Greenberg Traurig, USA

Brad is a member of the Health Care & FDA Practice in Greenberg Traurig's Philadelphia office. As a healthcare regulatory and transactional attorney, Brad represents a range of clients in the health sector including hospitals, health plans, medical practices, pharmacies, patient assistance programmes, electronic health records providers, management companies, pharmaceutical manufacturers and medical device companies. He regularly advises clients on virtually all aspects of health information privacy and security compliance under the Health Insurance Portability and Accountability Act (HIPAA) and state law, and spends considerable time helping clients navigate the multi-speciality realm of digital health, including providing business structuring advice to facilitate pursuing desired operational outcomes without running afoul of regulatory constraints. Brad also has deep experience guiding clients through significant privacy and security incident response and associated investigations. Brad's experience also includes assisting hospitals on arrangements with physicians, such as joint ventures, physician recruitment, practice acquisitions and employment arrangements, as well as compliance with federal and state laws governing referrals among healthcare providers, such as the Anti-Kickback Statute and the Stark Law. Brad also advises clients in a variety of areas including the corporate practice of medicine, facility licensing, hospital/medical staff relationships, informed consent and regulatory compliance in the operation of Medicare, Medicaid and other third party reimbursement programmes.

Logan Square, 1717 Arch Street, Suite 400, Philadelphia, PA 19103, USA
Tel: +1 215-972-59363; E-mail: brad.rostolsky@gtlaw.com

Abstract On 26th April, 2024, the Federal Trade Commission (FTC) issued a final rule amending the 2009 Health Breach Notification Rule (HBNR). The primary aim of the Final Rule is to close gaps between the preceding version of the FTC's breach notification rule and the protections offered by the breach notification regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The FTC focused on the

personal data regularly processed by direct-to-consumer Health Apps, which represent a growing segment of the healthcare industry not regulated by HIPAA. This paper provides an in-depth analysis of the changes introduced by the Final Rule, the implications for businesses not regulated by HIPAA, and the potential operational ripple effects for many businesses now regulated under the Final Rule. It also discusses the updated individual notification obligations and the need for impacted individuals to be made aware of potential risks while balancing issues related to notice fatigue.

KEYWORDS: Health Breach Notification Rule, Federal Trade Commission, personal health records, HIPAA, data privacy, mobile health apps

DOI: 10.69554/JXUY4255

INTRODUCTION

On 26th April, 2024, the Federal Trade Commission (FTC) issued a final rule (Final Rule) amending the 2009 Health Breach Notification Rule (HBNR). Aiming to close the gaps (both perceived and real) between the preceding version of the FTC's breach notification rule and the protections offered by the breach notification regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the FTC largely took aim at the ever-growing list of mobile health applications (collectively, Health Apps) that had managed to avoid any federal breach notice obligations. In particular, the FTC focused on the personal data regularly entered and stored in direct-to-consumer Health Apps, which are representative of a growing segment of the healthcare industry not regulated by HIPAA. Clarifying that Health Apps are within the FTC's purview through its amplification of key definitions within the Final Rule, the FTC's reimagination of the HBNR should come as no surprise to those paying attention to the FTC policy statement in September of 2021.[1] Specifically, the Final Rule's definition of personal health record (PHR) now clearly applies to Health Apps and connected devices that are (merely) capable of drawing information from multiple sources.

FORESHADOWING THROUGH SETTLEMENTS

Prior to publishing the Final Rule, the FTC gave a preview of the rule's ultimate revised content through the agency's settlement with GoodRx and Easy Healthcare Corporation. In both instances, the settlements leant heavily on the FTC's 2021 guidance and the companies' offerings would probably not have qualified under the original HBNR's definition of PHR. With respect to GoodRx, a widely used telemedicine platform that, among other things, offers consumers coupons for discounts on prescription medications, the FTC concluded that the company improperly shared individuals' sensitive health information with third parties (including Facebook and Google) for advertising purposes without first obtaining consumer authorisations.[2] In particular, the FTC focused on the fact that the company shared this information in contravention of its published privacy statements. In addition to imposing civil penalties, the FTC notably: (a) called out the company's failure to comply with all aspects of the HBNR's notification requirements; (b) prohibited GoodRx from sharing user health data with certain third parties for advertising purposes and (c) required GoodRx to direct third parties to delete the consumer health data at issue.[3]

The FTC quickly followed its first-ever HBNR enforcement action with another against Easy Healthcare Corporation (Easy Healthcare), which the FTC characterised as having committed failures similar to those of GoodRx in terms of consumer transparency. The FTC determined that Easy Healthcare, through its ovulation tracking mobile device application, Premom Ovulation Tracker (Premom), effectively deceived consumers about the company's data sharing practices.[4] In addition to alleging Section 5 violations stemming from Easy Healthcare's sharing of individuals' sensitive personal and health information with third parties contrary to the company's stated privacy policies and without having received affirmative express consent, the FTC took the position that Easy Healthcare, like GoodRx, failed to notify individuals about the unauthorised disclosures in violation of the HBNR.[5] Also like GoodRx, Easy Healthcare was (a) required to seek deletion by certain third parties of the personal data at issue; and (b) was prohibited from sharing user personal health data with third parties for advertising purposes.[6] In both enforcement actions, the FTC found the disclosures to third party advertisers of health-related personal data to *constitute a breach* under the HBNR and the failure to notify impacted individuals to be a *violation* of *HBNR*.

Notwithstanding that it took the FTC 11 years to enforce the HBNR, it is apparent from these two settlements, in combination with the 2021 policy statement — and now the Final Rule — that the sharing of individuals' sensitive health information must meet the rigour of the FTC when HIPAA does not apply. Businesses not regulated by HIPAA will no longer be scrutinised only under Section 5 and applicable state law, and the FTC has made it clear that stakes are high. Consent decrees imposing fines and changes to compliance practices are now being bolstered by penalising violators in a new way — requiring the deletion of personal data given to third parties and prohibiting businesses from using this personal data for certain revenue-generating purposes.

THE FINAL RULE VERSUS THE 2009 HBNR

A summary of the differences between the Final Rule and the 2009 HBNR can be found in Table 1. For this paper's purpose, the focus will be on the key changes in definitions and obligations that significantly alter the landscape for entities not clearly in scope of the 2009 HBNR.

KEY DEFINITION CHANGES

The most significant changes within the Final Rule have been accomplished through the FTC's modifications to the HBNR's core definitions. And, to that end, because the primary aim of the HBNR was to make it clear that Health Apps and other web-based health businesses not regulated under HIPAA would need to notify consumers when their health information had been breached, the Final Rule does just that.

The Commission clarified that 'PHR identifiable health information' includes

> traditional health information (such as diagnoses or medications), health information derived from consumers' interactions with apps and other online services (such as health information generated from tracking technologies employed on websites or mobile applications or from customized records of website or mobile application interactions), as well as emergent health data.[7]

The Final Rule, through the amended definition of PHR identifiable health information, also formally broadened how regulated entities should view the term 'health care provider' by creating the term 'covered health care provider', which now includes an expansive category for 'any other entity furnishing health care services or supplies'.[8]

Table 1: Summary of changes to HBNR

Aspect	2009 Rule	Final Rule
Definition of breach of security	Not clear that a voluntary disclosure, unauthorised by the consumer, made by a PHR vendor or PHR related entity counted as a breach.	Clarifies that a breach of security includes unauthorised acquisition as a result of a data breach *or* an unauthorised disclosure.
Definition of covered healthcare provider	No definition.	Includes any entity 'furnishing health care services or supplies'.
Definition of healthcare services or supplies	No definition.	Includes websites, mobile apps and Internet-connected devices that provide health-related services or tools, eg apps that track medical issues (medications, fertility) or wellness (fitness, sleep, diet).
Definition of personal health record	Defined as an electronic record of PHR identifiable health information *that can be drawn from multiple sources*.	Changes language to 'has the technical capacity to draw information from multiple sources' to clarify that an app with technical means to draw information from multiple sources (based on the app's programming) is a PHR even when customer chooses not to use those features.
Definition of PHR identifiable health information	Defined as information that is provided by or on behalf of an individual and identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual.	Removes a cross-reference and broadens definition to cover health information derived from consumers' interactions with apps and online services, as well as emergent health data, eg health information inferred from location and purchases.
Definition of PHR-related entity	Defined as an entity that offers products or services through a *website*.	First, clarifies that definition includes entities that offer products and services through *online services*, such as apps, not just websites. Second, narrows third prong to entities that access or send *unsecured* PHR identifiable health information.
Notification requirements	Only requires notice to individuals and FTC.	Adds that vendors of PHR and PHR related entities must now notify media outlets of a state or jurisdiction following discovery of breach if impacting 500 or more of its residents.
Timing requirement	Required notice to FTC no later than 10 business days following date of discovery of breach. § 318.5(c).	For breaches involving 500 or more people, need to notify FTC at same time notice is provided to individuals, third party service providers and media;[1] if fewer than 500 people, need only notify FTC annually.[2]
Method of notice	Requires notification by first-class mail.[3]	Allows notification by electronic mail[4] if specified as primary method of communication.
Content of notice	Required brief description of what happened, description of type of unsecured PHR identifiable health information involved, steps individual should take to protect themselves from harm, description of what entity is doing to investigate and mitigate harm and one contact procedure.	Now also requires full name or identity of third party that acquired the PHR identifiable health information,[5] a more detailed description of unsecured information involved in the breach, description of what notifying entity is doing to protect individuals and two or more contact procedures.

(*Continued*)

Table 1: Summary of changes to HBNR (*continued*)

Aspect	2009 Rule	Final Rule
Penalties/ Enforcement	Treated as violation of Federal Trade Commission Act; subject to civil penalty of approx. $50,000 per violation.	No change.

[1] Without unreasonable delay and no later than 60 calendar days after discovery of breach.

[2] No later than 60 days following end of calendar year.

[3] Unless individual is given clear, conspicuous and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice.

[4] Defined as e-mail in combination with one or more of the following: text message, within-application messaging or electronic banner. See § 318.2.

[5] Except where providing the full name or identity of the third party would pose a risk to the affected individuals or the entity providing notice. Then a description is sufficient.

The Final Rule now definitively applies to many businesses that had been viewed as out-of-scope for the HBNR, such as those that leverage mobile applications and the Internet of Things to provide wellness offerings, like the makers of a smartwatch that syncs to applications providing health-related feedback. The FTC made clear that it views as within its regulatory purview essentially all non-HIPAA regulated individually identifiable health information to the extent it is connected to an FTC regulated entity.

To this end, the agency's modification of the definition of 'PHR related entity' broadly encompasses entities that are not covered by HIPAA that interact with a PHR vendor by offering products or services via their or a vendor's website (or any online service) or by accessing identifiable health information in a PHR or sending identifiable information to a PHR.[9] In explaining the proposed clarification, which was later adopted, the Commission identified 'remote blood pressure cuffs, connected blood glucose monitors, and fitness trackers as examples of internet-connected devices that could qualify as a PHR related entity when individuals sync them with a personal health record (e.g., a health app)'.[10]

However, this was contrasted with the example of a grocery delivery service that sends information about food purchases to a diet/fitness app — such an entity would not be considered a PHR-related entity if the grocery delivery service does not access/send unsecured PHR identifiable health information in/to a personal health record.[11]

Unlike most of other changes, the FTC's minor change to the proposed definition of 'health care services or supplies' was made in an effort to limit a broader-than-intended understanding of the term. Specifically, 'health care services or supplies' has been redefined and now:

> means [not 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*.[12]

While the Commission intended to provide clear boundaries on what constitutes 'health care services or supplies', by removing the prior catch-all provisions of 'any other entity furnishing health care services or supplies' and replacing it with the above italicised language, it is not clear that the regulators accomplished the intended clarification. Would the maker

of an alcohol breathalyser that syncs data through a mobile app be considered a covered healthcare provider because the connected device arguably tracks someone's diet and/or provides insight into one's alcohol consumption? Would the maker of the original Fitbit be considered a covered healthcare provider even though the original device only tracked steps, and steps alone are arguably not indicative of fitness?

As set forth in the FTC's proposed regulation, a 'breach of security' no longer merely encompasses what people typically think of as data security breaches. The term now includes intentional and unauthorised disclosures and uses. The Commission explained that under the updated definition, a breach may occur where data is obtained for one legitimate purpose, but later used for a secondary purpose that was not originally authorised by the individual. Whether a disclosure or use is authorised requires an analysis of the context of the interaction between the individual and the business, the nature of the disclosure or use, the recipients of the data (as applicable), the purpose of the disclosure, the businesses' representations to the individual (ie the privacy notice) and other applicable laws.[13]

There will surely be future discussions about whether someone's authorisation can be implicitly provided. More specifically, the Commission's decisions here have two particularly notable impacts. One, 'the unauthorized access or use [in and of itself] of derived PHR identifiable information may also constitute a breach of security.'[14] Relatedly, the Commission made the decision not to define the term 'authorize' or 'authorization'. This, in combination with the Final Rule's emphasis that for certain types of access there will be a rebuttable presumption that unauthorised access has occurred, may cause significant operational ripple effects for many businesses now regulated under the Final Rule.

KEY OBLIGATION CHANGES

The key definitional changes noted above directly affect compliance obligations for entities who were already in scope for HBNR and for those that are now regulated under the Final Rule. If an entity is: (1) HBNR-regulated; (2) PHR identifiable information is accessed, used or disclosed by a third party without authorisation; and if unsecured PHR identifiable health information is provided to a third party, the entity may have experienced a breach under the Final Rule and will have notification obligations. The key here, however, is to recognise that the entity needs to act to determine if it has these obligations.

Additionally, the Final Rule provides more proscriptive requirements for the timing, content and way the notification is provided:

Notification to impacted individuals. The notice of a breach of security must include:

- a description of what happened, including the name or identity of any third parties that acquired the unsecured PHR identifiable health information due to the breach of security, unless providing the name or identity of that third party would pose a risk to individuals or the notifying entity — in that case, a description of the acquiring third party is sufficient;[15]
- a description of the types of unsecured PHR identifiable health information involved in the breach of security;[16]
- a description of what the notifying entity is doing to prevent further breaches and protect impacted individuals (eg investigatory and remedial actions)[17] and
- two methods by which an impacted individual can contact the notifying entity to learn more about the breach of security, specifically toll-free phone number, e-mail address, website, in-app or postal address.[18]

The updated individual notification obligations attempt to weigh the need for impacted individuals to be made aware of

potential risks, while balancing issues related to notice fatigue. Impacted individuals may now receive notification in a manner that reflects their online interactions with the notifying entity instead of only by postal mail. The notification may be delivered to impacted individuals via electronic mail (clarified in the final rule as e-mail along with text message, within-application message or electronic banner) if the impacted individual already consented to receive electronic communications and the notice is conspicuous.[19] Notably, the Commission did not adopt a proposal to include a description of the potential harms an impacted individual might experience as a result of the security breach.[20] Instead, the FTC believes that by requiring notifying entities to describe the types of unsecured PHR identifiable health information involved in the breach of security, impacted individuals will be better equipped to 'understand the risks they face'.[21]

Notification to the FTC. The FTC should receive the same information sent to the impacted individuals at the same time the impacted individuals are notified. Mirroring the HIPAA Breach Notification Rule, the Final Rule also obligates regulated entities to notify the FTC on the same timeline as impacted individuals — 'without unreasonable delay' and in no case later than 60 calendar days after the discovery of a security breach involving 500 or more individuals.[22] The Commission cautioned against using 60 days as the intended timeline stating that '60 days should serve' as the outer limit.[23]

A summary of the key changes in the Final Rule can be found in Table 1.

ADVISING WHEN AMBIGUITY REMAINS

Despite the Commission's efforts to clarify the scope and requirements of the HBNR with the Final Rule, there are several points with which privacy subject matter experts will be wrestling unless and until there is further interpretation. Understanding whether and how an entity is governed by the Final Rule is a crucial step in providing guidance for entities to comply with the Final Rule.

For example, an online retailer of a wide variety of consumer goods discloses personal data to a migraine tracking app including the individual's purchase history of certain vitamins, over-the-counter medications, ice packs for the face and head, anti-glare screen covers and other goods identified by the migraine tracking app as recommended at-home migraine care. The migraine tracking app collects information from its users regarding the frequency and severity of migraines, as well as what medications and other steps the user is taking to mitigate his/her migraines. The migraine tracking app also syncs with the users' smartwatches to collect health-related data to help the user understand correlations between specific metrics and the occurrence of migraines. How do we advise the online retailer of its likely risks and obligations under the Final Rule?

Because we know the Final Rule applies to vendors of PHRs, PHR-related entities and third party service providers for a vendor of PHRs or PHR-related entity, the first step in analysing the situation is to determine whether the personal data being processed constitutes a PHR. That requires two considerations: (1) determining whether there is PHR identifiable information; and (2) assessing whether that electronic record is technically able to draw from multiple sources by or on behalf of the individual.

Is there PHR identifiable information?

To advise the online retailer of its potential obligations under the Final Rule, the first step in analysis (assuming the data flow is confirmed and it has been determined HIPAA does not apply to the parties) is to assess whether the data

being processed is PHR identifiable health information. This requires reviewing several of the updated definitions in the Final Rule. The migraine tracking app is handling data at the end user's request that is related to the health condition of an identifiable user. For this information to be considered PHR identifiable health information, it must also be created or received by a covered healthcare provider, health plan, employer or clearing house. A 'covered health care provider' is not only a provider of medical or other health services, but also any other entity 'furnishing health care services or supplies'.[24] With the broadened definition of 'health care services or supplies',[25] it would be difficult to argue the migraine tracking app is not a covered healthcare provider as its intended use is to track migraines. Therefore, the data collected and processed by the migraine tracking app is very likely to be considered PHR identifiable information.

On the other hand, the online retailer is processing the personal data mentioned above in the context of offering goods to consumers via a website or app. Because the online retailer does not only offer migraine treatment (or other health/treatment related) goods, a strong argument could be made that this data is not 'more than tangentially related to' health. However, if this online retailer is collecting this dataset specifically to share it with the migraine tracking app, that argument may be undermined. If that were the case, we would want to proceed to the second prong of analysis and assess whether the electronic record could draw from multiple sources as mentioned above.

Is the online retailer a vendor of PHRs?

To be a vendor of PHRs, the online retailer must offer or maintain PHRs. Assuming the online retailer collects user purchase history data for goods, it is not offering or maintaining PHRs.

Is the online retailer a PHR-related entity?

The online retailer must meet one of the three criteria set forth in the PHR-related entity definition to qualify as one. While the online retailer does offer goods through an online experience, it does not offer products or services of a vendor of PHRs. The goods it sells are also unlikely to be considered products or services of a HIPAA covered entity that offers PHRs. Lastly, the online retailer does not access unsecured PHR identifiable information in a PHR or send unsecured PHR-identifiable health information to a PHR in the scenario provided above. Therefore, the online retailer is not a PHR-related entity.

Is the online vendor a third party service provider for a vendor of PHRs?

To address this question, we must address the role of the migraine tracking app, specifically whether it offers or maintains a PHR. The information processed by the migraine tracking app relates to a health condition of an identifiable individual and includes information that is provided by or on behalf of the end user. To be PHR identifiable health information, it must also be created or received by one of the enumerated entities. The nature of the migraine tracking app supports finding that it provides healthcare services. Further, the migraine tracking app is creating an electronic record about the end user's migraine experience from multiple sources: the smartwatch and from the online retailer. The fact we have an electronic record of PHR identifiable health information about the migraine tracking app end user that draws from these two sources, both of which are processed for the individual, means it is probable this will be considered a PHR. The migraine tracking app is maintaining this record, and therefore, meets the definition of a vendor of PHRs.

The nature of the data share from the online retailer to the migraine tracking

app will become important at this point. Again, if this is information the online retailer collects about its end users as part of its regular operations, there is not a strong argument that it is providing a service to the migraine tracking app. It is more likely to be characterised as a controller-to-controller scenario. On the other hand, if the online retailer is collecting certain data as instructed by the migraine tracking app, especially if it would not collect that data but for the migraine tracking app, that argument becomes much stronger. In either scenario, the online retailer would have to process unsecured PHR identifiable information because of the services to qualify as a third party service provider.

The online retailer can be advised of its applicable legal obligations under the Final Rule once it is determined whether the online retailer is a vendor of PHRs, a PHR-related entity or third party service provider for a vendor of PHRs.

RECONSIDERING LEGAL OBLIGATIONS

Data privacy practitioners will play a pivotal role in guiding entities on strategy and compliance. For entities that were already making efforts to comply with HBNR before these updates, a review of services/products, data inventories, data flows, privacy notices and incident response plans should be implemented to ensure the scope of the Final Rule has not crept into other areas of the business and that consumer-facing language and consent mechanisms would be defensible to the FTC. For entities new to HBNR, those same exercises will be necessary and will require additional work to create and execute an HBNR compliant programme. Key privacy programme aspects for all in scope entities to examine include determining whether the entity is a vendor of PHRs, PHR related entity or third party service provider and/or whether the entity could be labelled as more than one due to different data flows and roles to the individual and disclosing/receiving party. The entity may need to make updates to comply with new obligations, such as ensuring:

- individuals can consent in a meaningful way to the disclosure of their PHR identifiable health information;
- the entity's privacy notice accurately discloses the processing of PHR identifiable health information;
- individuals would reasonably expect that the entity is processing PHR identifiable information;
- the entity's applicable template breach notification is 'reasonably understandable' and clearly conveys the significance of the notification; and
- the delivery method for that breach notification aligns with how the entity interacts with individuals.

Additionally complicating matters will be the need to appreciate the extent to which HIPAA, state law and HBNR may apply to various service lines offered by a business. Privacy practitioners will have to work with key stakeholders in understanding the client's goals, risk appetite and current state of its privacy programme to help their clients navigate the updated HBNR. This will remain challenging until there is additional guidance from or enforcement actions by the FTC.

References

1. Much of the Final Rule stems from the sentiments offered in the policy statement of the Federal Trade Commission (15th September, 2021) 'On Breaches by Health Apps and Other Connected Devices', available at https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf (accessed 9th June, 2024).
2. See, Federal Trade Commission (1st February, 2023) 'FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for

Advertising', available at https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising (accessed 9th June, 2024).
3. *Ibid*.
4. See, Federal Trade Commission (17th May, 2023) 'Ovulation Tracking App Premom will be Barred from Sharing Health Data for Advertising under Proposed FTC Order', available at https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc (accessed 9th June, 2024).
5. *Ibid*.
6. *Ibid*.
7. Federal Trade Commission (n.d.) 'Final Rule', 16 CFR 213, pp. 13–14, 105, available at https://www.ftc.gov/system/files/ftc_gov/pdf/p205405healthbreachnotificationrule.pdf (accessed 9th June, 2024).
8. *Ibid*., p. 105.
9. *Ibid*., pp. 63, 106; see also Federal Trade Commission (2024) 'Complying with FTC's Health Breach Notification Rule', available at https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0 (accessed 9th June, 2024).
10. Federal Trade Commission, ref 7 above, p. 59.
11. *Ibid*., p. 59.
12. *Ibid*., p. 105. Emphasis added.
13. *Ibid*., p. 49.
14. *Ibid*., p. 58.
15. *Ibid*., p. 82.
16. *Ibid*., p. 83.
17. *Ibid*., p. 83.
18. *Ibid*., p. 85.
19. *Ibid*., pp. 71–2.
20. *Ibid*., p. 81.
21. *Ibid*., p. 83.
22. *Ibid*., p. 88.
23. *Ibid*., p. 88.
24. Federal Trade Commission (n.d.) 'Health Breach Notification Rule', p. 104, available at https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule (accessed 9th June, 2024).
25. *Ibid*., p. 105, specifically, 'Health care services or supplies means any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools'.