Massachusetts Health Data Consortium

FTC Health Breach Notification (FTC-2023-0037-0001) Comment

This document is submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) in response to the FTC Health Breach Notification (FTC-2023-0037-0001) NPRM posted in the Federal Register on June 9, 2023 and found here: https://www.federalregister.gov/documents/2023/06/09/2023-12148/health-breach-notification-rule

About MHDC

Founded in 1978, MHDC, a not-for-profit corporation, convenes the Massachusetts's health information community in advancing multi-stakeholder health data collaborations. MHDC's members include payers, providers, industry associations, state and federal agencies, technology and services companies, and consumers. The Consortium is the oldest organization of its kind in the country.

MHDC provides a variety of services to its members including educational and networking opportunities, analytics services on both the administrative and clinical side (Spotlight), and data governance and standardization efforts for both clinical and administrative data (the Data Governance Collaborative/DGC and the New England Healthcare Exchange Network, respectively).

About DGC

The DGC is a collaboration between payer and provider organizations convened to discuss, design, and implement data sharing and interoperability among payers, providers, patients/members, and other interested parties who need health data. It is a one stop interoperability resource. The DGC primarily focuses on three areas:

1. Collaboration: Development of common understanding of and specifications for data standards, exchange mechanisms, and what it means to participate in the modern health IT ecosystem
2. Education: helping members understand their regulatory obligations, the data and exchange standards they're expected to use, and modern technology and related processes
3. Innovation: Identification and development of projects and services needed to make modern health data practices and exchange a reality

General Comments

This section comments on the general approach taken by the FTC in their posted proposal or comments on items that cross multiple sections of the proposed rule

Exhibit A

The proposed rule references Exhibit A which is supposed to be a model notice for public comment but this exhibit does not appear to exist within any form/format of the rule we've been able to find (downloaded PDF, on the Federal Register website, on Regulations.gov, etc). We look forward to an opportunity to review and comment on this model notice in the future.

Comparison to Current State and How Definitions Tie Together

We commend the FTC for providing useful background information on the rule, its intent, and its history and for providing some comparisons for individual suggested changes. However, if the FTC puts forth a similar proposed rule in the future (with a lot of deltas from existing language and definitions), we urge the agency to

consider providing a cohesive framework of how they fit together for more direct and complete comparison. We struggled at times to understand exactly how all of these definitions fit together into a cohesive whole representing what is and is not acceptable behavior by different entities according to the existing rule and how the new rules fit together to change that.

This was exacerbated by the order in which definitions were presented. Definitions that relied on understanding non-standard definitions outlined later in the proposed rule were difficult to understand when presented. For example, the definition of PHR identifiable information relies on the non-standard definitions of health care provider and the non-standard definition of health care services that follows. Without those later definitions the first definition does not make sense and does not fulfill the stated goal of the first definition as outlined in the rule. For people reading and reacting to the rule linearly (as we did) this meant we spent time crafting a response indicating why the definition did not meet those stated goals before we ever reached the later, clarifying additional definitions.

Need for Public Education

Participants in our Data Governance Collaborative note that common thoughts about what is and is not health or health-related data have changed over time and a 70 year old may have a very different idea about this than a 30 year old. Educating the public on what formally constitutes health data, what is officially considered a security or privacy breach, and similar topics related to the concepts of this rule is going to be an important part of the overall strategy of consistent reporting of violations and subsequent enforcement.

Development of a Formal Vendor Contract Requirement for Data Handling

As part of our discussion of vendors that support health-related websites, mobile applications, and other technology covered by this rule, our DGC participants felt that a formal framework of requirements that pass legal obligations around data practices to the subordinate vendors is necessary to ensure the protection of the consumer's data. They envisioned a mechanism like that of Business Associate Agreements used under HIPAA to ensure that organizations do the right thing and that provide legal teeth and real enforcement mechanisms for things like self-reporting breaches.

This was deemed particularly important given that many of the activities resulting in breaches under the formal definition may be the result of preferred business practices of the vendor organizations (selling data to advertisers, providing data to analytics vendors without protections that it will not be used for other purposes or resold, etc.). Unless organizations have incentive to actually stop choosing to employ those practices and to report them when they are employed, they are likely to continue unabated.

Using Non-Standard Definitions of Common Terms

This may be driven in whole or in part by requirements of the underlying legislation, but it is disconcerting at best and confusing at worst to redefine common terms like healthcare provider or electronic mail for the purposes of this rule (we may discuss specific cases in more detail below). These terms are generally accepted to have a specific meaning and reusing them to mean something else here is problematic. If this is being done because it's the only way to fit this regulation into the underlying laws then we understand, but ask that the FTC call this out so people at least understand why they're being asked to accept some of these odd, non-standard definitions.

Consumer Visibility into Data Sharing

One component of consumer health data control is allowing the consumer to see everywhere their data is shared. We believe that any affirmative agreement for sharing should involve transparency and a requirement that a consumer be able to easily see a record of which data was shared with which organizations at which time for what purpose. Consumers should be able to flag suspect sharing they did not believe they gave consent for and have the consent trail tracked/presented/investigated/reported as appropriate.

In addition, there should be some mechanism for revoking consent previously given if a consumer no longer wishes to allow the related data sharing and the requirement that all data sharing cease within a short timeframe after the revocation (and immediately if possible).

Definition of unsecured health information

We found it notable that in an NPRM that spends so much time defining relevant terminology, a definition of unsecured health information is never provided. We believe this oversight should be corrected.

In addition, it is unclear why this term is important for most of the workflows and use cases discussed by this proposed rule. While unsecured data is bad and unsecured health data is worse, breaches of health data will occur regardless of whether the data is considered secured or unsecured (they are just more likely when unsecured) and we do not feel any rules related to what constitutes a breach or the responsibilities for obtaining consent for certain data sharing should be dependent on whether data is considered secured or unsecured. Providing the context regarding why this term is needed and how it impacts the rules/expectations of application, vendor, or consumer behavior would be extremely helpful.

We do note that the term is used in HIPAA and perhaps it is an artifact from those definitions, but if intended to be a comment primarily on the encryption level of data while it is being transported and stored, we note that this may be pertinent to some extent for traditional security breaches but it is not particularly pertinent to disclosure-related breaches which are a primary focus of this rule.

Health Information Inferred from Non-Health Data

The FTC is somewhat inconsistent across the proposed rule regarding its treatment of data that can be used to infer health information about a consumer and, at times, about the health information inferred from such data. We urge the commission to clarify its intent in this area and consistently ensure that all definitions and other components of the rule are explicitly clear about this intent. Source data that is not health information but could be used to infer it should be directly included or excluded from definitions as appropriate in keeping with a clear, consistent viewpoint. Similarly, inferred health information should be clearly and consistently addressed whenever appropriate.

Including the Chain of Custody of Data in Breach Notices

We applaud the FTC requirement that the breach notice come from the PHR vendor that a consumer directly interacts with and not any of their vendors or subordinate organizations that may actually be responsible for the breach. One of the poorer consumer experiences of the HIPAA breach notification process is that such notices come from the business associate breached and in many cases consumers do not have any idea how that organization got their data in the first place or, sometimes, even what data/which covered entity's data they had and was breached.

However, we still feel it is important for the consumer to understand which organization was responsible for the actual breach to help understand which organizations they wish to trust with their data in the future. Thus, the full chain of custody of the data and how it came to be held by the organization that either shared it without authorization or was the victim of a more traditional security breach should be part of the consumer notice about any breach.

Considerations for non-health apps that import health information

Participants in our Data Governance Collaborative thought it important to explicitly address the use case where a non-health application imports or otherwise acquires health-related information. For example, a calendar that imports schedules containing medical appointments or wherein a consumer manually enters medical appointments is not a health-related app but it contains personally identifiable health information. Consumers may not think of a calendar app as a health app. Being explicit about how these types of cases are treated by the health data breach rule is an important aspect of consumer (and app developer) education on the rule.

GDPR approach to consent

Participants in our Data Governance Collaborative believe it is potentially onerous for consumers to have to individually review every data sharing event but still want each one bound by the same rules. In addition to a general Business Associate Agreement type framework like the one used in HIPAA as discussed in a previous comment, some of our participants favor a GDPR-style approach which allows individuals to generally opt-in or opt-out of certain types/categories of data sharing or to pick and choose what data is shared and how it is used

instead of requiring individual consents for each sharing action.

We note that this type of approach might raise the bar to entry for third party applications and small developers as it can be complex to implement and maintain.

Data Resale

Participants in our Data Governance Collaborative universally oppose the ability for an entity to reshare or sell data that was shared to them with consumer consent without acquiring another direct consent from the consumer (outside of a BAA-type framework and then only if the sharing is to directly support business operations essential to the performance of the application, website, etc).

Medical Device data

We note that there are prescribed medical devices that patients might expect to fall within HIPAA that do not and would be covered by this rule instead. One example of this is the extensive patient data collected by a CPAP machine for individuals with obstructive sleep apnea. This is a prescription-only device used in the home, but the data collected is “owned” by the device manufacturer and not protected by HIPAA. The data use policies of most of the manufacturers are not consumer-friendly and, in general, many people who use these devices are unaware specific data about their sleep patterns is being collected at all, let alone being shared without their permission. Explicitly calling out examples of this sort and discussing how the rule applies would be helpful to consumers and manufacturers alike.

Solution for Regulating Health Data at Non-Profits

As a non-profit, MHDC is aware that the FTC does not have authority over non-profit organizations, but many consumers do not understand this. It leaves a major loophole for consumer protections in that health data held by non-profits not covered by HIPAA are not covered by any other regulatory authority.

We realize it is not the FTC’s responsibility to solve this issue, but some solution is needed to ensure proper, comprehensive consumer protections for their identifiable health information regardless of who holds it or their organizational status.

Response to Specific Questions – Clarification of Entities Covered

This section will list specific questions asked about the clarification of entities covered in the proposal and our responses to them.

The Commission requests comment as to whether any further amendment of the definition [of PHR identifiable information] is needed to clarify the scope of data covered.

This was one of the definitions that initially perplexed us because it relies on subsequent definitions of health care provider (which in turn relies on other definitions that follow it).

Once those subsequent definitions are considered, this definition covers the majority of cases you specifically call out as wanting to ensure are covered. However, we question whether all of the emergent health data cases are adequately covered in the definition. We also wonder if there are some inconsistencies between the desire to include this information in the definition and later statements in other sections of the rule related to intentions around grocery purchase information and similar.

We would like to see the FTC explicitly clarify what types of data and what types of data originators are covered by the rule and be consistent about that throughout. We understand that there is no one easy answer when it comes to things like recent purchase histories or location data or health-related books read via an online ebook/audiobook purchasing or borrowing application (to list but a few scenarios), but as noted in the intent of this definition, it is absolutely clear that these are just three among many types of data that can – but

may not always – contain personal health information.

Some of this data is further complicated by being tied to a household rather than an individual. Purchase data may cover an individual or an entire household. In the latter case, it will tell you someone in the household is buying over-the-counter asthma medication but not necessarily which resident. It only becomes personally identifiable when tied to other data, such as when grocery store purchases are fed into a mobile app or website with a specific logged in user. Even then, it's possible that the user is not able to distinguish between "mine" and "not mine" (or doing so is too onerous) so they just accept the erroneous data and move forward if they don't see it as interfering with the reason they're using the app.

Again, we do not know exactly where the line should be drawn or what the right answer is. In general, we would lean toward covering more data than absolutely necessary rather than accidentally omitting health data that a consumer would want protected. We also feel the single most important criteria is a clear, consistent, and comprehensible definition applied universally so everyone understands what the rules are.

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.

We believe the same rules should apply to any technology that otherwise meets the definition. For example, if a smart refrigerator tracks when food is removed and by whom, that should be considered wellness/diet information and treated just like the data collected from a mobile app tracking what someone eats. If the display includes advertising, the consumer should not have their diet/food purchase data shared without permission in order to better personalize the advertising. Similarly, if data is stored in the cloud and analyzed by a vendor to note trends, the data should either be de-identified first or the consumer should have to explicitly consent to this use.

We agree with the FTC position that a small checkbox at the end of a long EULA or data use document or privacy policy should not constitute affirmative consent for any use – they should have to explicitly ask for consent to share for a specific purpose and/or with a specific organization. They should be able to see and affirmatively consent to any relevant data use policies at the secondary organizations and/or have to explicitly consent to any secondary/additional data sharing performed by those organizations they agreed could have their data.

If the scope should be limited, the Commission seeks comment as to how that limitation could be effected through the Rule's language

We believe that the FTC should be more explicit that de-identified data is excluded from this rule but also be very clear about what constituted de-identified data and how to handle de-identified data that could easily be re-attached to an individual because of their specific circumstances or for some other reason.

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.

We note that even here the FTC is slightly inconsistent. This request for comment is followed immediately by:

"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."

But the descriptions and explanations of intent in the main section above this request for comment section is more expansive than this, explicitly noting that the rule is meant to incorporate emerging health data such as recent purchase data or location data. In general, as noted above, there is inconsistency in exactly what the intended coverage is throughout the proposed rule. We ask the FTC to be more consistent per our previous comments.

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 that limitation could be effected through the Rule's language

Again, we ask for clarification on the intent of the coverage. We believe that the coverage should be broad and should err on the side of being more protective rather than less. For example, while it is possible that someone working nearby chooses to eat lunch at the Dana Farber Cancer Institute cafeteria twice a week, it is more likely that someone who isn't a known employee doing so is a patient or a caretaker of someone with cancer and this information could be used for all sorts of purposes that violate that person's privacy. A better example in today's environment is the tracking of individuals whose phone location data place them within 200 feet of an abortion clinic and the use of such data to harass, subject the individual to unpleasant investigations, or otherwise cause them harm of some sort. We believe this data should be protected and only available with consent or under legal compulsion. Similarly, purchasing an over the counter narcotics rescue medication might cause someone to infer that the purchaser takes narcotics either legally or illegally which could lead to a variety of unexpected and unpleasant consequences including harassment, employment-related inquiries or even firing, or negative assumptions about the purchaser. The examples are numerous and consumers should be protected from these types of inferred conclusions whether they turn out to be accurate or not.

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 pharmacies)

As noted above, we are not fans of redefining a term with a commonly accepted definition solely within the context of this rule. We would prefer the use of an additional term to reference mobile app developers, website owners, and other entities that fit your adjusted definition but not the traditional definition of health care provider. One possible alternate term might be "health information provider" or "health support provider" (as distinguished from a care provider). We note that we have no issue with using the term health care provider for personnel providing traditional health care services via an application interface (such as a mental health application that provides counselling from a licensed psychiatrist or psychologist or a telehealth application employing a cadre of nurse practitioners to provide direct services to its users) or for the applications themselves if that is their sole purpose.

If the addition of another term is not possible for a technical reason (such as constraints from the underlying law) then the FTC should explicitly use this as rationale for the existing definition.

The Commission seeks comment on the definition of "healthcare services or supplies," including whether any modifications should be made to this definition.

We believe the inclusion of wellness information could be made more explicit by adding the following bolded text to the existing definition supplied in the NPRM:

"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- **or wellness-**related services or tools."

That said, in keeping with our other comments, we would prefer the use of a different term for this concept rather than re-using a standard term normally given a different definition. However, we do not have a proposed alternative and we find this definition more acceptable than the health care provider changes outlined elsewhere and could live with the definition (preferably with the small edit noted above).

If the addition of another term is not possible for a technical reason (such as constraints from the underlying

law) then the FTC should explicitly use this as rationale for the existing definition.

Response to Specific Questions – Clarification Regarding Types of Breaches Subject to the Rule

This section will list specific questions asked about the clarification of types of breaches covered in the proposal and our responses to them.

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

While we do not feel this addition is necessary, in general we feel it is always better to be explicit so we favor its inclusion. That said, we do see one potential downside: that some entities will feel that because there's an explicit change to include unauthorized acquisition of data that it was not verboten before.

We also wonder about the inclusion of the word unsecured in the definition (see general comment above). We would expect this definition to apply to all health data regardless of how well it is secured.

Response to Specific Questions – Revised Scope of PHR Related Entity

This section will list specific questions asked about the revised scope of PHR Related Entity covered in the proposal and our responses to them.

The Commission seeks comment on whether additional changes to the Rule would be necessary or helpful to clarify this result.

As noted in the general comments above, we feel the grocery store purchase data is a poor example, one that would meet the definition of what the FTC noted it intended to cover (recent purchase information) in earlier definition.

For example, if someone buys products aimed at diabetics or if someone buys entirely gluten free it could be indicative of a medical issue and not just a lifestyle choice. Further, OTC medical products are frequently purchased at grocery stores and it seems fraught to make a distinction between where the data is being sent and/or how the incoming data is being used/exactly which subset of available data is being requested to determine if a rule applies.

Clarity and consistency on this issue is needed. We understand that this is a difficult area to clearly define. In some ways it is a slippery slope where more and more data gets classified as health-related and becomes subject to this rule. However, we feel that a more expansive definition is better than one that is too restrictive and allows unapproved movement of health-related data without any recourse or right to complain about the behavior.

Our Data Governance Collaborative had a lengthy discussion trying to sort out where we felt the line should be and to a person we all fell on the "restrict as much as possible" end of the spectrum but could not come up with a cohesive, consistent, clear, and comprehensible definition that makes sense for this. As one participant stated "no one needs to know what I bought at Target: the best way is to not use an app, pay in cash, etc. but that's impractical so how do we get a handle on this?"

While we have made our preferences clear, we feel that as long as the FTC sets a clear definition and uses it consistently across the entire rule then a minimum acceptable bar is met.

Please comment on the following scenario: A consumer gives permission for PHR data collection. A third party services provider receives PHR identifiable

health info. They sell it to someone else without consumer consent. The third party services provider must notify the vendor. The vendor must notify the individual

The FTC explicitly asked if the consumer should be notified in this scenario. Our DGC provided a unanimous, unambiguous loud yes. However, we question the idea of a third party services provider self-reporting their own deliberate bad behavior in this scenario unless they are subject to strict contractual obligations with severe penalties in case of failure (analogous to a HIPAA BAA; see general comment above).

Even without this extra level of protection, we feel there should be some obligation on the part of the original collector of the data given the direct consumer consent to ensure that the data use policies and practices of its vendors comply with the expectations of the consumer. For example, in this scenario, the original vendor should have some responsibility for the actions of its services provider. In addition, depending on the consent they received from the original consumer it might be reasonable to expect an additional level of consent before the data was sent to the third party services provider. In that case, the original vendor is definition on the hook and exhibited bad behavior that should be considered a rule violation for giving the third party services provider the data and perhaps a second violation for the third party's resale of the data.

We also feel some level of auditing should be both available to and required by the original entity given consent to share data with all of the downstream entities given access to the data based on the original consent. The consumer trusted that entity to follow the rules outlined in the consents given and the entity should be able to enforce those rules on other organizations that are acting on its behalf.

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

As noted above, we do not understand the inclusion of the word unsecured and will ignore it for the purposes of the rest of this comment. We believe the change to the first portion of the definition makes sense but the change to the third prong is likely not the correct way to address this issue. We do not have any issue with the existing third prong, but if the FTC feels additional clarification is needed this is not the correct form for it.

Response to Specific Questions – Clarification of What it Means for a Personal Health Record to Draw Information from Multiple Sources

This section will list specific questions asked about drawing information from multiple sources covered in the proposal and our responses to them.

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.

The modifications to the definition to explicitly reflect that the capacity for multiple sources of data is the necessary criteria and not the actual use of multiple sources is clear. However, the proposed definition could be improved by explicitly noting that only one of the data sources needs to explicitly (potentially) include patient health information to qualify.

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)

From a consumer perspective, requiring multiple sources of health information does not make sense. If something has health information (or the capacity to have health information) then it should be treated as such and have health data-related privacy protections. Whether that information came from one, two, or twenty sources is not particularly relevant.

or only draws *identifiable* health information from one place (in addition to non-identifiable health information drawn elsewhere)

Similarly, it doesn't particularly matter to a consumer if the information is originally identifiable health information at its source if it becomes so within an application or device receiving that data. Any application or digital device with personal health information should be covered in an ideal world. For example, an application that uses generic geographic likelihood of disease prevalence information in combination with personal demographic information to present "likelihood of the user contracting X disease in the next N years" type information is generating all of its personally identifiable health information within the application but that does not make the data any less worthy of protection than an app that starts by pulling in such estimates as calculated 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.

We believe the capacity to draw information is a good criterion. Having to track the actual usage of data would be onerous and having to reach a threshold of usage means that some consumers will have identifiable health information that isn't covered by the rule which we feel is problematic, especially if they expect any health data held by third party applications outside of HIPAA are protected by FTC rules and make choices accordingly.

Response to Specific Questions – Facilitating Greater Opportunity for Electronic Notice

This section will list specific questions asked about using electronic notice of breaches covered in the proposal and our responses to them.

This model notice is attached as Exhibit A to this Notice of Proposed Rulemaking. The Commission invites comment on this model notice

Unfortunately it does not appear that this model notice was attached to the NPRM in any format (in the Federal Register, on Regulations.gov, downloaded PDF, etc). We would welcome future opportunity to examine and comment on a model notice.

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

We strongly urge the FTC not to use this definition of electronic mail. Electronic mail is email and email is electronic mail and trying to use the term to mean anything else is extremely problematic.

If possible, defining another term such as electronic notification method should be used. We feel even more strongly about redefining electronic mail than we do about other terms and feel it should not be done unless

there is no way to meet FTC needs any other way.

If the addition of another term is not possible for a technical reason (such as constraints from the underlying law) then the FTC should explicitly use this as rationale for the existing definition.

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.

We feel that duplication for the sake of duplication should not be required. However, a consumer should be able to select multiple electronic mechanisms for notification if so desired (allowing separate opt-in/consent for each).

Further, we note that the different mechanisms listed in the proposed rule are not equivalent – some are push notifications that a consumer is likely to see without directly interacting with the application, website, or device and some require consumer interaction with the application, website, or device in order to see the notification.

We strongly recommend that the requirement be selection of one push notification but that additional options like in-app notifications and website banners be supported as additional, secondary notice options. In fact, the FTC might consider requiring that all breach notices be publicly posted on a website or be available within an app as a separate requirement outside of direct, individual consumer notification.

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.

In theory, if requiring two electronic notification methods, this may happen. However, if you require individual opt-in for each method and only require consumers to supply the data needed to support the options they choose then this should be limited.

Perhaps the final rule could note that the expectation is contact information will only be collected for notice mechanisms the consumer opts to use unless that contact information has been supplied for some other reason.

Response to Specific Questions – Expanded Content of Notice

This section will list specific questions asked about the expanded content of notice covered in the proposal and our responses to them.

whether the requirement that the notice describe potential harms would serve the public interest and benefit consumers

While explaining to consumers why they should care about a breach seems sensible and there is no question many individuals will not understand the implications of a breach without explanation, any such explanations will almost certainly be incomplete or best guesses at the most likely outcomes. By providing such explanations as the potential harms some individuals may take them as the only possible harms that could occur and not be on the lookout for other possible consequences.

On the whole, we do feel including some potential harms would be helpful, but feel like requiring language stating they are only some of the potential harms or that other consequences may also occur is important to limit the assumptions that the actions outlined in the notice are the only possible bad outcomes from the breach.

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

We are categorically opposed to stating there are no known harms that may result from a breach solely because a notifying entity is unaware of any specific bad outcomes. This gives a false level of comfort to the affected consumers. We believe that a general statement such as “we are unaware of any specific harms from this breach at the time of this notice but that does not mean none exist now or in the future” or similar. We do not want to unnecessarily alarm anyone, but feel that putting someone on notice to be vigilant is greatly preferable to pretending everything is fine without any real knowledge this is the case.

Further, allowing entities to indicate they know of no specific harms at the time of a notice may encourage them not to look for potential harms that may be easily discoverable because they don’t want to report them in the related notice.

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

In addition to the type of statement outlined in the previous comment directly above this one, we feel a general list of potential harms from a few common types of breaches may be appropriate. For instance, a traditional active security breach may result in data being sold to bad actors on the dark web, identity theft, or use of healthcare erroneously attributed to the consumer for billing and/or medical history purposes to name just a few. Selling data to an advertiser may result in cold sales calls from random companies, erroneous identification of health conditions the consumer doesn’t have, or misinformation that others act upon in various ways to name a few.

We suggest picking the 3-4 most common types of breaches and outlining some standard “some but not all of the possible consequences include” lists that should be used when more specific information is not available.

whether additional and more specific data elements may overwhelm or confuse recipients of the notice.

We do not believe the type of data being discussed in this proposed rule is overkill or likely to overwhelm or confuse the average consumer if presented factually and with the proper context. We believe it is better to err on the side of transparency and disclose as much as possible.

If there are real concerns in this direction, perhaps a required shorter “overview” section at the top of a notice followed by all of the details for those who want them might be an appropriate way to address them. This would give folks an easy way to see the major takeaways but also the ability to have all of the pertinent data if they wish to have it.

Response to Specific Questions – Defining Authorization and Affirmative Express Consent

This section will list specific questions asked about authorization and affirmative express consent covered in the proposal as considered but not adopted and our responses to them.

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.

While there likely is enough guidance to put companies on notice, particularly given the existing enforcement actions, we still believe being explicit about the expectations for authorization and consumer consent is

appropriate.

In particular, we feel it is essential to make it clear that nominal consent acquired via a small checkbox at the end of a privacy policy, data use policy, or terms of service is not sufficient consent to meet the affirmative express consent bar, especially if the box is checked by default (but even if it is not).

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?

This should be acceptable, but only if the button is encountered within the natural workflow of performing a related task and if the purpose of the sharing and some mechanism for reviewing/seeing the data being shared prior to accepting the option. Clicking “enable diet analysis” or “share data to enable diet analysis” or “share data with X company” should not be sufficient, something like “share entered food log data and any integrated grocery purchases with X company to enable diet analysis” should be required.

If enabling sharing generally, when first configuring an application, or upon opening an app for the first time/first time after an upgrade, a description of each option should be required and they should all start unchecked.

In both cases, if the consumer is agreeing to allow further downstream data sharing that should be captured and encapsulated within the original consent request.

These rules could possibly be loosened/be less stringent if a system similar to BAA agreements was enabled (see previous comments related to this) that placed downstream organizations under strict data use rules.

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?

We do not believe a general terms and conditions statement should be sufficient consent for data sharing. They could be bundled together into categories/full workflows to limit the burden, but each type of data sharing should be explicitly outlined to the consumer and require their consent (barring a BAA-like environment).

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?

We do not believe any data sharing information within a privacy policy should be sufficient consent for data sharing on its own, although outlining some general policies and approaches to data sharing would be helpful and appropriate. They could be bundled together into categories/full workflows to limit the burden, but each type of data sharing should be explicitly outlined to the consumer and require their consent (barring a BAA-like environment).

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.

We cannot think of any off the top of our heads, but note that even should some exist, having them listed as partners or users of the consumer data is still important for transparency. Further, consumers should be able to decide they don’t trust certain organizations with their data and decline to share with them even if that means they cannot use a specific mobile application or website that relies on that organization for an essential service.

Response to Specific Questions – Modifying Definition of Third Party Service Provider

This section will list specific questions asked about the third party service provider definition covered in the proposal as considered but not adopted and our responses to them.

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?

In a word, yes.