UnitedHealth Group℠

Ann E. Tobin, JD
Senior Privacy Counsel
UnitedHealth Group
9900 Bren Road East, MN008-T700
Minnetonka, MN 55343

June 1, 2009

Federal Trade Commission/Office of the Secretary
Room H-135 (Annex M)
600 Pennsylvania Ave., N.W.
Washington, D.C. 20580

Re: Health Breach Notification Rulemaking, Project No. R911002

Dear Sir or Madam:

UnitedHealth Group is pleased to provide the Federal Trade Commission ("FTC") our comments on the proposed regulations regarding the breach notification requirements relating to personal health records ("PHRs") published in the *Federal Register* on April 20, 2009 ("Proposed Rule"). [1]

UnitedHealth Group has grown to become one of America's most innovative suppliers of health care solutions by focusing on ideas that help improve medical outcomes while reducing health care costs. We serve the health care system itself, across the care community. The people we serve have made us a national leader in health benefit programs. The core of our business and social mission is to help people live healthier lives. We do this by continuously delivering innovations that significantly improve the way America's health care system works. We apply careful analysis to a large collection of health care data to solve complex problems, to develop practical technology for both providers of care and consumers, and to advance financial and operational connectivity across the system.

We use our resources and expertise to support consumers, patients, care providers, employers, and benefit sponsors, so that they can make more informed health care decisions. Our breadth of services and leadership in both private and public programs enable us to adapt to a constantly evolving environment in order to make health care more accessible, affordable, and personalized. As one of America's leading health care companies, UnitedHealth Group serves

[1] 74 Fed. Reg. 17,914 (April 20, 2009).

more than 70 million Americans each year. Partnering with more than 650,000 physicians and other care providers, 5,200 hospitals, 80,000 dentists, and 65,000 pharmacies in all 50 states, we touch nearly every aspect of health care delivery and financing.

UnitedHealth Group is committed to protecting the privacy of the individuals we serve. We believe that the manner in which the FTC implements these regulations on the breach notification requirements is very important to safeguarding consumer information. UnitedHealth Group supported the American Recovery and Reinvestment Act of 2009 ("ARRA"), including the Health Information Technology for Economic and Clinical Health Act set forth in Title XIII of ARRA (the "HITECH Act"). UnitedHealth Group fully supports FTC's efforts to implement the Proposed Rule in a manner that provides vendors of personal health records ("PHR vendors") and similar entities that are not covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") with clear guidelines for securing PHR identifiable information. UnitedHealth Group is both a covered entity and a business associate under HIPAA, and in those capacities we sometimes contract with vendors of personal health records. We also have subsidiaries that themselves operate as vendors of personal health records – in this capacity, these subsidiaries may be (i) a business associate to a UnitedHealth Group covered entity; (ii) a business associate to a non-UnitedHealth Group related covered entity; or (iii) as detailed below, in a relationship with an individual independent of any relationship with a health plan. Therefore, as a company that includes some divisions that may be subject to the FTC breach notification provisions, while the core of our business – our health plans – will fall under the parallel provisions governed by the Department of Health and Human Services ("HHS"), we believe it will be important that the FTC breach notification regulations and the corresponding HHS regulations affecting covered entities and business associates be consistent. We appreciate the agencies' efforts to make their respective breach notification regulations consistent.

UnitedHealth Group respectfully requests that FTC consider the following comments when finalizing the breach notification regulations.

I. Entities with a Dual Role as a PHR Vendor and a Business Associate

UnitedHealth Group appreciates the FTC's clarification that business associates of HIPAA covered entities are excluded from FTC jurisdiction when acting in the capacity as a business associate to a HIPAA covered entity. UnitedHealth Group includes subsidiaries that serve as business associates of covered entities and simultaneously offer and maintain PHRs outside of a business associate capacity. It is critical that any breach of the information maintained by these business units result in a single notification to consumers, rather than duplicate notification. Under the HHS requirements, business associates already are obligated to notify covered entities of a breach.[2] If business associate activities also were subject to the FTC breach notification rules, the business associate, as PHR vendor, arguably would be required to separately notify the affected consumers of the same breach in order to comply with the FTC

[2] ARRA, Pub. L. No. 111-5, § 13402(a), 123 Stat. 115, 260 (Feb. 17, 2009).

requirements. We believe that Congress did not intend such a result, and we support the FTC's clarification of jurisdiction for business associates.

UnitedHealth Group seeks clarification regarding the appropriate jurisdiction when an individual discontinues use of a PHR that was supported through a covered entity. For example, an individual may choose to maintain a PHR that is offered through his or her health plan via a PHR vendor that serves as a business associate to the health plan. If the individual later disenrolls from the health plan, perhaps due to a change in employment, the individual may be permitted to continue to use the PHR by establishing an independent relationship with the PHR vendor. When the PHR is accessed through the individual's relationship with the health plan, through the health plan's business associate, any breach would seem to clearly fall within the jurisdiction of HHS. Once the individual has disenrolled from the health plan, however, the health plan maintains no further relationship with the individual, and thus notification from the health plan of a breach would not seem appropriate. Instead, once the individual has established an independent relationship with the PHR vendor, we would expect that the information maintained in that PHR would be subject to the FTC rules in the event of a breach. We are seeking clarification that the FTC has jurisdiction once the PHR is no longer available through a covered entity or business associate.

UnitedHealth Group also requests that the FTC provide similar guidance with respect to Health Information Exchanges ("HIEs"), entities that may collect, store, and/or exchange individually identifiable health information. HIEs play an increasingly important role in the development of a national health information network, and many states have established or are in the process of establishing HIEs. HIEs may serve as business associates of covered entities and may also receive information directly from PHR vendors. Depending on the model, a HIE may combine the information it receives from various sources into a single file containing all information on an individual, or may maintain information received from different entities separately. As a company that seeks to facilitate the success of HIEs and thus a national health information network, UnitedHealth Group would appreciate guidance from the FTC regarding when a HIE should be considered a business associate. In particular, we would welcome examples of when different models of HIEs should be treated as a business associate and the breach notification rules – either those promulgated by the FTC or by HHS – that should apply.

II. Definitions – Proposed § 318.2

A. Breach of Security – Proposed § 318.2(a)

UnitedHealth Group supports the FTC's proposed definition of a "breach of security"[3] and, in particular, appreciates the rebuttable presumption that unauthorized acquisition includes unauthorized access unless the entity experiencing the breach "has reliable evidence showing that there has not been, or could not reasonably have been, any unauthorized acquisition

[3] Proposed § 318.2(a).

of such information."[4] We seek clarification, however, that PHR identifiable health information has not been acquired where there is no reasonable likelihood of harm to an individual.

Using the FTC's example of possible scenarios in which information may have been accessed versus acquired, where an employee inadvertently accessed a database, realizes that it is not the database he or she intended to view, and logged off without reading, using, or disclosing any information, we agree that the information was not acquired and no breach occurred.[5] Even if the employee read part of the file, however, before determining that it was the wrong database, and subsequently followed appropriate internal procedures for addressing such access, such as notifying a supervisor or complying with internal reporting procedures, we believe that the information was not acquired for purposes of the breach notification rules.

The new federal breach notification requirement is intended to alert individuals of breaches of their information so that they may take precautions to mitigate harm. Indeed, the statute requires the federal breach notification to include "the steps individuals should take to protect themselves from potential harm resulting from the breach."[6] For example, this may include advising recipients to take actions such as closely monitoring credit reports and explanation of benefits statements to guard against fraud or medical identity theft. Providing notice to individuals for whom there is no reasonable likelihood of harm may create needless anxiety among the recipients of the notices and does not appear to be consistent with the statutory intent.

Notifying individuals for whom there is no reasonable likelihood of harm also may ultimately result in more harm than if notice had not been provided, particularly in the case of large-scale breaches that must be reported to the local media under the federal breach notice provisions. By publicizing the incident and the nature of the breach, identity thieves and other criminals may be alerted to the incident and capitalize on an opportunity to defraud the affected individuals. Publicizing that individuals who maintain PHRs with a particular vendor may have had their information compromised may make those individuals more vulnerable to fraudulent schemes. For example, if it is widely known that the information regarding members of a particular health plan who maintain PHRs may have been breached, that public knowledge may make it easier for criminals to locate sensitive information that was part of the breach and use that information as part of an identify theft scheme. The publicity also may make it more likely that individuals whose information was subject to the breach will be targeted by criminals offering false credit monitoring and other fraudulent services as a means of accessing personal information. Given the goals of the breach notification requirements and the possible negative consequences of notifying individuals where their information was accessed without resulting harm, we believe that such notification should not be required when it serves no real benefit to the individuals notified. We encourage the FTC to clarify that a "breach of security" has not

---

[4] *Id.*
[5] 74 Fed. Reg. at 17,915.
[6] ARRA at 13402(f).

occurred where a PHR vendor determines that there is no reasonable likelihood of harm to an individual as a result of the breach.

B. PHR Related Entity – Proposed § 318.2(f)

UnitedHealth Group requests that the FTC clarify that the definition of "PHR related entity"[7] encompasses only entities that, as part of their routine business operations, electronically access PHRs or knowingly send information to PHRs. We are concerned that the third component of the proposed definition of "PHR related entity", which includes an entity that accesses information in a PHR or sends information to a PHR, may be too broadly construed. For example, an individual PHR consumer may authorize another individual or entity (including family, friends, or personal care representatives) to access his or her PHR information electronically. We do not believe that either the statute or the Proposed Rule intend to require the FTC to regulate these types of persons or entities that access PHRs in these situations. We urge the FTC to modify this portion of the definition to clarify that a "PHR related entity" includes entities that electronically access information in a PHR or knowingly send information to a PHR as part of routine business operations. This would appropriately protect consumers by exercising jurisdiction over entities whose business operations pertain to PHRs without unduly obligating individuals or entities that have incidental contact with a PHR through permission of an individual to comply with the breach notification provisions. Should the FTC decline to make such a clarification, we request that the FTC explain what types of entities this third part of the definition is intended to include.

III. Notice to and Acknowledgement from a Senior Official – Proposed 318.3(b)

The FTC has proposed that a third party service provider notify a senior official at the PHR vendor of a breach of security as well as obtain an acknowledgement that the senior official has received the notice. UnitedHealth Group is concerned that the requirement that a third party service provider obtain an acknowledgement of receipt of the notice is unnecessary and may slow down the more important work that needs to be done to address the breach. This proposed acknowledgement requirement may divert time and resources that the PHR vendor could be using to send prompt notifications to individuals and otherwise comply with the breach provisions. Instead, we recommend that the requirement, if any, be limited to reasonable proof that the notice was sent to an address of record. For example, a certified letter receipt from the U.S. Postal Service, or a record of an e-mail successfully sent should be sufficient.

[7] Proposed § 318.2(f).

IV. Timeliness of Breach Notifications – Proposed § 318.4

With respect to the FTC proposal that breach notification be provided to individuals without unreasonable delay but in no case later than 60 calendar days after discovery of the breach,[8] UnitedHealth Group requests that the FTC specify that the 60 day clock begins when the entity discovers that the individual's information is involved in the breach. This approach would ensure that PHR vendors that experience a breach would provide notice to those individuals actually affected by the breach in compliance with the breach notification requirements.

In many cases it may take the full 60 days or longer to determine the scope of a breach and who must be notified. For example, one could envision a situation where an entity may initially determine that a data breach is isolated to certain computerized records containing the PHR identifiable health information of 100 individuals, and would be able to notify those individuals well within the 60 days; after further investigation continuing beyond 60 days, the PHR vendor may discover that the breach actually extended to another record set and it involves the PHR identifiable health information of well over 500 individuals requiring notice not only to the individuals but also to prominent media outlets serving the relevant states and to the FTC. The notices provided to the other individuals after the 60 day clock had expired technically could be interpreted as not in compliance with the 60 day requirement, even though the entity had not yet discovered the breach of those individuals' information. In order to ensure compliance with the 60 day requirement in this type of situation, there is the risk that an entity would instead over-notify individuals, providing notice to the entire universe of individuals who *may* have been affected. These notices would create needless anxiety and confusion among the individuals receiving them, particularly when the entity could not say with certainty which, or if any, elements of their information were breached. In order to avoid technical violations of the 60 day requirement as well as to avoid over-notification of individuals whose information turns out not to have been breached, we request that the 60 day clock begin at the point at which a PHR vendor learns that an individual's records were in fact breached.

V. Notice to Individuals – Proposed § 318.5(a)

Section 13402(e)(1)(B) of ARRA requires notice of a breach through conspicuous posting on the entity's website or publication in major print or broadcast media "in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information."[9] We believe that the FTC's interpretation of this provision is not consistent with the statutory language. Instead, the FTC requires such website posting and publication in print

---

[8] Proposed § 318.4(a); *see also* ARRA at 13402(d)(1).
[9] ARRA at 13402(e)(1)(B).

or broadcast media if "ten or more individuals *cannot be reached* by the [specified] methods."[10] We are concerned that the FTC's proposed language may imply that a PHR vendor or PHR related entity has an obligation to confirm that the notice provided to individuals affected by a breach has been received. ARRA expressly permits written notice by first-class mail and does not require that entities providing individual notice confirm receipt. We believe the statutory language is more appropriate, and we respectfully request that the FTC revise proposed § 318.5(a)(4) accordingly. In addition, we request that FTC make clear in the final rule that in circumstances where a PHR vendor or PHR related entity does not have sufficient contact information to notify an individual directly, it is the entity rather than the FTC that elects which method to use to provide notice (i.e., through conspicuous posting on the entity's website or publication in major print or broadcast media).

VI. Notice to Media – Proposed § 318.5(b)

We appreciate the FTC's proposed language in § 318.5(b), which closely tracks the statutory requirements regarding media notice for breaches of security involving the unsecured PHR identifiable health information of 500 or more individuals. As with the statutory provision, the FTC's proposed regulation requires notice "to prominent media outlets serving a State or jurisdiction." We are concerned, however, that the FTC's preamble discussion of this proposed provision[11] may suggest media notice beyond the notice to "prominent media outlets" required by the statute and proposed by the FTC. In some states or localities, notice to a range of broadcast and print media may be appropriate and necessary in order to comply with the breach notification requirements. In other areas affected by the breach, such as rural areas or states, the required media notice may be accomplished by dissemination of a press release to the single newspaper covering the area as well as to the area's major television networks. We ask that the FTC recognize that the provision of notice to prominent media outlets necessarily will vary by area and clarify that an entity may be considered in compliance with these requirements where it has properly notified prominent media outlets in the affected area.

VII. Notice to the FTC and Annual Breach Logs – Proposed § 318.5(c)

Notice to the FTC. In proposed § 318.5(c), the FTC has interpreted the statutory requirement of "immediate" notice to the FTC for breaches affecting 500 or more individuals to mean "as soon as possible, and in no case later than five business days."[12] While we appreciate that the FTC needs prompt notice of large scale breaches and that ARRA requires immediacy, we are concerned that requiring PHR vendors and PHR related entities to notify the FTC within 5 business days following the date of discovery of the breach will not permit these entities to conduct a proper investigation, particularly with respect to breaches that appear to be large scale

---

[10] Proposed § 318.5(a)(4) (emphasis added); *see also* 74 Fed. Reg. at 17,918- 17,919.
[11] 74 Fed. Reg. at 17,919.
[12] *See also Id.*

and to which this requirement applies. Where an entity has enough information to determine that a breach of unsecured information has occurred and that the breach relates to 500 or more individuals, 5 business days may be an acceptable standard. In many cases, however, an entity will not have the information necessary to make this determination within 5 business days, and a longer time period for notification to the FTC may be more appropriate.

In order to meet the FTC's proposed deadline, PHR vendors and PHR related entities would have to submit a notice based on the information gathered in the first 5 days of investigation, which may be incomplete or even inaccurate. As a result, entities will likely need to provide several and possibly conflicting follow-up notices as more information becomes available. For example, an entity may become aware of a potential breach of security that may involve the information of 500 or more individuals and notify the FTC within the proposed 5 business days; upon further investigation, however, the information may turn out to have been encrypted and thus no breach of security in fact occurred. In this situation, a longer time period for notification to the FTC would have avoided the need to report to the FTC what was in essence a false alarm. We believe that a longer period of notice for larger breaches would still meet the statutory requirement for immediacy while giving entities sufficient time to make an initial determination that a breach of security had in fact occurred. Therefore, we propose that the final regulations require entities to report any breach that affects 500 or more individuals to the FTC no later than 30 calendar days after discovery of the breach incident in circumstances where the entity does not have sufficient information to make a determination as to whether the information was secured.

Another possible scenario is that an entity discovers a breach that appears to involve the records of 100 individuals. Here, the entity may properly record the breach in the annual log for later submission to the FTC but then, after the 5 business days proposed by the FTC, discover that the breach of security involved more than 500 individuals. As discussed in Section IV, above, we urge the FTC to clarify that a breach of security is considered discovered when an entity becomes aware that an individual's information has been breached. This clarification would ensure that entities are not out of compliance with the requirement for notice to the FTC as long as they provide such notice within the required number of days from the date of discovery that the breach of security involved 500 or more individuals. Therefore, we urge the FTC to revise § 318.5(c) to require reporting to the FTC within 5 business days following the PHR vendor's or PHR related entity's determination that the breach of security involves 500 or more individuals.

Annual breach logs. UnitedHealth Group appreciates the FTC's proposal regarding when the annual log of breaches involving fewer than 500 individuals must be submitted but we think that the proposal set forth in proposed § 318.5(c) is not sufficiently specific to ensure consistent compliance. The FTC has proposed that the annual log "shall be due one year from the date of the entity's first breach."[13] Instead, UnitedHealth Group requests

[13] 74 Fed. Reg. at 17,920.

that the FTC establish a single reporting date for entities required to submit such a log to the FTC. Establishing one annual date for all such entities, rather than a rolling date based on an entity's initial breach, will minimize confusion and facilitate compliance. For example, the FTC could require affected entities to submit a log for breaches occurring during a calendar year within a certain period after the end of the year. UnitedHealth Group also requests that the FTC implement this statutory provision in a manner that allows PHR vendors and PHR related entities to report breaches to the FTC as a single corporate entity, rather than requiring each subsidiary or separate business unit of the entity to individually submit a report.

VIII. State Law Conflicts and Proposed Resolutions

We have highlighted below some specific requirements of state law that are different than the federal requirements. For at least one state – Massachusetts – this means that compliance with both state and federal law is not possible. In other states, these different laws mean that the federal notice would not easily satisfy notice obligations in those states. We urge the FTC to provide guidance on the preemption of contrary state laws, as well as to clarify that the federal notice requirements are not exclusive and that entities may incorporate state law requirements that are not preempted into a single notice. We also request the FTC's guidance on when state notice may be required but where the information was encrypted in accordance with federal requirements.

A. Circumstances Where Required Federal Notice Would Not Satisfy State Notice Obligations.

UnitedHealth Group encourages the FTC to incorporate the federal preemption provision at Section 13421(a) of ARRA into the final rule. Such guidance is needed to assist PHR vendors and PHR related entities when assessing state breach notification obligations that are in direct conflict with the federal breach notice requirements. Section 13421(a) of ARRA states that the preemption requirement set forth in the HIPAA statute, Section 1178 of the Social Security Act, also applies to the provisions of Subtitle D of ARRA, including the breach notification provision applicable to PHR vendors and PHR related entities. Applying that standard, the federal breach provision would preempt any contrary requirement of state law.[14] UnitedHealth Group urges the FTC to construe the term "contrary" to mean that a PHR vendors and PHR related entities could not comply with both federal and state breach notification requirements.

---

[14] There are certain exceptions to the HIPAA preemption standard. *See* 42 U.S.C. § 1320d-7(a). For example, if the state law at issue relates to the privacy of individually identifiable health information, then the preemption standard is different. A state privacy law is not preempted unless it is contrary to a provision of the Privacy Rule promulgated by HHS and is less stringent than the federal privacy provision. *See* Section 264(c)(2) of Pub. L. 104-191 and as a note to 42 U.S.C. § 1320d-2.

As an example, it would be impossible for PHR vendors and PHR related entities who experience a breach of PHR identifiable health information that contains a sensitive identifier considered "personal information" under the Massachusetts security breach law (*e.g.*, social security number or financial account number) to comply with both the federal and Massachusetts laws with respect to the content of notice to affected individuals. In fact, compliance with the federal law would violate one of the notification requirements of the Massachusetts law. The Massachusetts law requires that the notification "shall not include the nature of the breach or unauthorized acquisition or use,"[15] while Section 13402(f) of ARRA states that the federal breach notification must include a description of the breach. Other state law conflicts may be resolved with a single notice that incorporates all of the elements required by the federal and state law, but the Massachusetts requirement to not disclose the nature of the breach does not allow for this compromise. Accordingly, we believe this type of requirement should be deemed contrary and thus preempted.

B. Other Potential Areas of Conflict Between Federal Breach Notification Requirements and State Breach Notification Laws.

The federal breach notification requirements apply to breaches of "unsecured" PHR identifiable health information. The majority of the state security breach laws do not apply to breaches of health information alone. Instead, the state laws generally apply to breaches of "personal information" which is commonly defined to include name in combination with sensitive identifiers such as social security number, drivers license or other state-issued identification number and financial account number (e.g., credit or debit card number). Despite this difference, the state law obligations are relevant for PHR vendors because the information maintained by these entities regularly includes identifiers such as social security numbers. Therefore, a breach of PHR identifiable health information could implicate state laws in many if not most circumstances, and UnitedHealth Group would like to highlight significant areas of conflict between the federal breach notification requirements and state breach notification laws that may arise in these circumstances.

Section 13402(f) of ARRA specifies content requirements for the federal breach notice, including: (1) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (2) a description of the types of unsecured PHR identifiable health information that were involved in the breach; (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number.

While these requirements are generally consistent with the state security breach laws, there are some notable distinctions. Some states require that a notice provide an individual

[15] Mass. Gen. Law. c. 93H, § 3 (emphasis added).

with specific advice about reporting suspected incidents of identity theft to law enforcement.[16] Others require advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.[17] Finally, several states require the notice to include the contact information for all major national consumer reporting agencies, and other states may require that specific state government contact information be included as well.[18]

We think that there is strong support for an interpretation by the FTC that state laws that are contrary to the federal breach requirement are preempted, as discussed above. For circumstances where a state law is not preempted, we urge the FTC to stipulate in the interim final regulations that the required content for federal breach notices is not exclusive and that the notice may include information in addition to what is set forth at Section 13402(f) of ARRA. By doing so, PHR vendors would be able to ensure that in most cases, both federal and state requirements are satisfied through one communication to the affected individual. The proposed clarification would reduce the administrative burden of issuing two separate letters – one that complies with federal law and one that complies with state law requirements in the state where the individual resides. It would also reduce anxiety and confusion among the individuals to be notified who may mistakenly think that multiple letters mean that there was more than one breach of their PHR identifiable health information.

C. Potential for Need to Send Multiple Notices to An Individual Upon Discovery of a Single Security Breach.

As described above, some states have very specific requirements for the content of breach notices that would result in multiple notices if the state-required elements were not preempted or could not be included in a federal notice. We have requested that the FTC stipulate in the interim final regulations that the required elements of the federal breach notice are not exclusive, which we view as essential to enable covered entities who must comply with both federal and state laws, to send a single notice to an individual in the event of a breach involving PHR identifiable health information.

We also strongly encourage the FTC to affirmatively declare that federal law permits combining notices. What is important is that an individual whose PHR identifiable health information is compromised due to a breach is notified so that he/she can take necessary precautions to mitigate the effect of the breach. As long as all the requirements of both laws are satisfied, a single notice that contains the requirements of both federal and state law should be permitted. In fact, if individuals begin to receive multiple notices about the same breach, it likely will create unnecessary confusion.

---

[16] Iowa and Oregon.
[17] Hawaii, Michigan, North Carolina, Vermont and Virginia.
[18] Iowa, Maryland, Oregon and Wyoming.

D. Circumstances Where an Entity Would Still Be Required to Notify Individuals of a Breach of Information that has been Rendered Secured Based On Federal Requirements.

All of the state laws require notice of a breach only if (i) it involves unauthorized access to and/or acquisition of personal information that was not encrypted or not rendered unreadable or unusable by any other method or technology or (ii) it involves unauthorized access to and/or acquisition of encrypted personal information and the confidential process or key to decrypt it. Therefore, in most circumstances a PHR vendor would not be required to notify individuals of a breach of information if that information was rendered secured based on the federal requirements of encryption or destruction. However, there may be circumstances where state law would obligate a vendor of personal health records or PHR related entity to notify individuals of a breach where the information has been encrypted and thus secured based on federal standards of encryption if the state law imposes a different standard of encryption. UnitedHealth Group requests clarification from the FTC on how PHR vendors should address such circumstances.

IX. Conclusion

UnitedHealth Group appreciates this opportunity to provide you with our comments on the Proposed Rule. Should you have any questions, please contact me at (952) 936-7236.

Sincerely,

Ann E. Tobin
Senior Privacy Counsel