

# Health Breach Notification Rulemaking

Project No. R911002

June 1, 2009

Donald S. Clark  
Secretary  
Federal Trade Commission

Dear Secretary Clark:

The Markle Foundation's Connecting for Health Initiative has since 2002 brought together leading government, industry and health care experts to accelerate the development of a health information-sharing environment to improve the quality and cost-effectiveness of health care. The Center for Democracy and Technology (CDT), through its Health Privacy Project, promotes comprehensive privacy and security policies to protect health data as information technology is increasingly used to support the exchange of health information. Together with Childbirth Connection, Health Care for All, the National Partnership for Women & Families, and the SEIU, we submit these comments in response to the notice of proposed rulemaking (NPRM) and request for public comment issued by the Federal Trade Commission (FTC).<sup>1</sup>

Section 13407 of the American Recovery and Reinvestment Act of 2009 (ARRA)<sup>2</sup> establishes temporary breach notification requirements for vendors of personal health records (PHRs)<sup>3</sup> and other entities not covered by the Health Insurance Portability and Accountability Act (HIPAA), and grants the FTC authority to issue interim final regulations governing these entities. Similarly, Section 13402 of ARRA imposes a new duty on entities covered by HIPAA and their business associates to provide notification to individuals when there has been a breach of "unsecured" protected health information (PHI). This latter provision applies to all

---

<sup>1</sup> The following additional people were consulted during several iterations of this draft. Their input was important to drafting these comments but their participation does not imply endorsement: Joy Pritts, Research Professor, Georgetown University; Michael Stokes, Policy & Compliance Director, Health Solutions Group, Microsoft Corporation; Carole Klove, Chief Compliance and Privacy Officer, UCLA Medical Sciences; Eric Cowperthwaite, Chief Information Security Officer, Providence Health & Services; and Gerry Hinkley, Partner, Davis Wright Tremaine LLP.

<sup>2</sup> Pub. L. 111-5, 123 Stat. 115 (2009).

<sup>3</sup> Defined in the statute as "an electronic *record* of PHR identifiable health information...on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." Section 13400 of ARRA (emphasis added).

protected health information (PHI) maintained by covered entities or their business associates, including information in PHRs.

With respect to both of these provisions, the term “unsecured” protected health information refers to PHI that is not secured through the use of a technology or methodology specified by the Department of Health and Human Services (HHS) in guidance as rendering the information unusable, unreadable, or indecipherable to unauthorized individuals.<sup>4</sup> HHS has recently issued guidance on this issue (the “HHS Guidance”), on which we have submitted separate comments.<sup>5</sup> Simultaneous with the issuance of the HHS Guidance, HHS published a request for information (RFI) in advance of its rulemaking to implement the breach notification provisions that apply to HIPAA covered entities and their business associates. We have also submitted comments on the RFI.<sup>6</sup>

The breach notification provisions in ARRA accomplish two important goals. First, they provide for individuals to receive notice in certain circumstances when their health information is at risk. Second, they create a powerful incentive for custodians of personal health information to adopt strong privacy and security practices in order to avoid a breach.

It is important to recognize the interaction of the rulemaking process being undertaken by FTC and HHS. FTC will promulgate breach notification rules that apply to PHR vendors and related entities. Breach notification rules promulgated by HHS will apply to HIPAA-covered entities or business associates of such entities. However, the rules to be issued by both HHS and FTC will set breach notification standards for PHRs. To avoid creating confusion for consumers, it is critical that PHRs be subject to consistent rules governing how they store and share consumer data.

Our comments below are mainly directed at achieving this consistent regulatory framework. We understand this issue will be broadly addressed in the forthcoming HHS and FTC privacy and security recommendations for PHRs, but we strongly recommend that HHS and FTC take this early opportunity to align policies and make them meaningful to consumers who must be able to navigate their use of PHRs.

In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information,<sup>7</sup> outlining consensus privacy and security policies for personal health records and other consumer access services. This framework—which was developed and supported by a diverse and broad group including technology companies, consumer organizations and HIPAA-covered entities<sup>8</sup>—was designed to meet the dual

---

<sup>4</sup> See Section 13402(h)(2) ARRA.

<sup>5</sup> See [http://www.connectingforhealth.org/resources/20090522\\_breach\\_methodologies.pdf](http://www.connectingforhealth.org/resources/20090522_breach_methodologies.pdf).

<sup>6</sup> See [http://www.connectingforhealth.org/resources/20090522\\_breach\\_provisions.pdf](http://www.connectingforhealth.org/resources/20090522_breach_provisions.pdf).

<sup>7</sup> See [www.connectingforhealth.org/phti](http://www.connectingforhealth.org/phti).

<sup>8</sup> See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at the following URL: <http://www.connectingforhealth.org/resources/CCEndorser.pdf>.

challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices.

A foundational principle of this work is that a consistent and meaningful set of policies for protecting information in personal health records is desirable for consumers, whether the PHR is offered by a HIPAA-covered entity or not. However, this does not imply that it is appropriate to simply extend HIPAA rules in their current form to uncovered entities supplying PHRs or new health information products. The approach of the Connecting for Health Common Framework was to develop a set of meaningful policies and practices that are appropriate for all entities that may provide consumers with personal health record services. With such services, consumers may keep electronic copies of personal health information and health-related transactions generated through their interactions with health entities, collected by health-monitoring devices, or contributed by themselves. Accordingly, another core principle of the Common Framework is that personal health records and other consumer access services are tools for consumers' use, and are controlled and managed by consumers.

It is critical that these basic consensus policies be considered in FTC's (and HHS') implementation of the new breach notification provisions. It will be confusing and potentially harmful to consumers to have different protections and rules for PHRs depending on the legal status or business model of the offering entity, and even more so if the policies do not consistently support meaningful consumer participation in and control of these emerging and powerful tools.

In summary, we urge FTC to:

- Work with HHS to apply consistent information and breach policies to PHRs in order to provide consumers with a reliable framework of protections;
- Ensure that individuals acting in a personal capacity are not considered to be a PHR related entity;
- Maintain its interpretation of the types of data that constitute PHR identifiable information;
- With respect to whether or not data is "identifiable," rely on HHS' Guidance<sup>9</sup> in determining whether or not data that has been breached is not at risk and acknowledge that the question of identifiability depends on the context;
- Presume that unsecured PHR identifiable information that is accessed by an unauthorized party is deemed to be "acquired";

---

<sup>9</sup> "Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under the HITECH Act," Federal Register/Vol. 74, No. 79/April 27, 2009.

- Ensure the breach definition is meaningful to individuals by setting parameters for authorization;
- Protect data in motion as well as at rest (and not just “in the PHR”);
- Add NIST SP 800-66 to the list of potential resources for reasonable security measures;
- With respect to the content of the notice to individuals, adhere to the statutory language and avoid imposing content requirements that could be a roadmap to lead to future breaches;
- Clarify which entities are accountable for notifying consumers in the event of breaches that may involve multiple parties.
- Revise the media notice requirements to specifically incorporate new media;
- Clarify timing issues with respect to notice to the FTC of breaches; and
- Support a study of state breach notification provisions to determine whether the new federal provisions conflict with existing state law, and whether state and federal laws will result in individuals receiving duplicate notices.

Finally, we agree that FTC’s determination that the temporary breach notification provisions in ARRA are an expansion of its authority under Section 5 of the Federal Trade Commission (FTC) Act.

### **1. FTC and HHS Should Apply Consistent Breach Notification Provisions to PHRs in Order to Provide Consumers with a Reliable Framework of Protections**

Personal health records hold significant potential for consumers and patients to become key, informed decision-makers in their own health care. By providing individuals with options for storing and sharing copies of their health records, as well as options for recording, storing, and sharing other information that is relevant to health care but is often absent from official medical records (such as pain thresholds in performing various activities of daily living, details on side effects of medication, and daily nutrition and exercise logs), personal health records can be drivers of needed change in our health care system.

In order to feel comfortable using PHRs, consumers need assurance that their information will be collected, used, or disclosed according to their preferences. It is reasonable for consumers to expect they will be able to authorize who may access any data they contribute or authorize to be contributed to any network-accessible PHR, and that they will be able to review audit logs of all disclosures of their records.

As noted above, one of the primary policies endorsed in the Markle Connecting for Health Common Framework for Networked Personal Health Information is that individuals should

have the choice of whether or not to open a PHR account, and individuals should choose what entities may access or exchange information into or out of that account.<sup>10</sup> This foundational policy is reflected in the definition of a PHR in ARRA: “an electronic record of information on an individual “that is managed, shared, *and controlled by or primarily for the individual.*”<sup>11</sup>

Section 13424(b) of ARRA requires HHS and FTC to report to Congress no later than February 18, 2010, with recommendations for privacy and security requirements for PHR vendors and related entities that are not covered by HIPAA as either covered entities or business associates. We urge FTC and HHS to refer to the Markle Connecting for Health Common Framework in developing its recommendations. It is not desirable to simply extend HIPAA in its current form and entirety to new entities without careful review of the policies and practices that may be appropriate to the specific instance of personal health records.<sup>12</sup> The Common Framework recommendations include policies and practices that are common to all entities, yet may be tailored to meet specific consumer expectations based on their relationship with the entities they chose to supply PHR services to them.

FTC and HHS should adopt consistent information and breach policies for PHR tools that give individuals the ability to input, store and control their own health information. FTC has proposed that breach notification for PHR vendors and related entities be triggered by acquisition of such information “without the authorization of the individual.” The rule’s focus on actions that are contrary to the individual’s specified choices with respect to their health information is appropriate. To ensure a consistent approach, in our comments to HHS’ April 17, 2009, request for information, we urged HHS in promulgating its breach notification rule to clarify that, with respect to a PHR offered by a covered entity or a business associate, the breach definition language “unauthorized acquisition, use or disclosure,” means acquisition, use or disclosure of protected health information “without the authorization of the individual.” We posit that this approach is required to appropriately implement ARRA’s definition of a PHR as being an electronic record of information on an individual “that is managed, shared, *and controlled by or primarily for the individual.*”<sup>13</sup> We believe FTC and HHS should interpret “breach” consistently for PHRs to include actions that are contrary to the individual’s authorization in order to achieve consistent regulation of PHRs regardless of the type of entity sponsoring or providing them.

## **2. Ensuring Individuals Acting in a Personal Capacity Are Not Considered to be a PHR Related Entity**

In its proposed rules, FTC specifically asks for comments on the nature of entities to which

---

<sup>10</sup> See <http://www.connectingforhealth.org/phti/reports/cp3.html>.

<sup>11</sup> Section 13400 of ARRA (emphasis added).

<sup>12</sup> See <http://www.cdt.org/healthprivacy/HIPAA-PHRs.pdf> for a more detailed explanation of why the HIPAA regulations in their current form are inappropriate for protecting consumers using PHRs.

<sup>13</sup> Section 13400 of ARRA (emphasis added).

the rules would apply, and the particular products and services they offer. The PHR marketplace is still very new, and the products and services being offered by and through PHRs are innovating rapidly. ARRA defines a PHR as an “electronic record of PHR identifiable health information...on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.”<sup>14</sup> It is critical that FTC remain flexible in applying this definition to accommodate the tools and services already on the market that meet this definition, as well as those that will be made available to consumers in the future.

With respect to PHR-related entities—those entities described in clauses (ii), (iii), and (iv) of Section 13424(b)(1)(A) of ARRA—we have some concerns that description in clause (iv) could be read to sweep in individuals acting in a personal capacity who “access information in a personal health record or send information to a personal health record.” For example, this description could be read to apply to family members who input material in and out of a PHR that belongs to kin. In most cases, only family members with authorization from the PHR account holder will be accessing information in a PHR; however, there may be circumstances where such authorization is withdrawn but the withdrawal is not fully processed or recognized by the PHR, and a technical “breach” may have occurred. FTC may want to clarify that the use of the term “entity” in that particular clause refers only to organized businesses and not individuals acting in a personal capacity.

### **3. Definition of Breach**

#### **A. “PHR Identifiable Information”**

In its notice of proposed rulemaking, FTC offered clarification regarding the definition of “PHR identifiable health information” contained in proposed section 318.2(e).<sup>15</sup> In addition to items such as names and credit card information when they are part of information contained in a PHR, FTC made clear that the definition includes the fact of having a PHR account with a PHR vendor or related entity when the products or services offered through the PHR indicate a particular health condition. We believe this interpretation is consistent with the statute; but, as noted in more detail below, we also encourage a context-based view of what determines identifiability.

#### **B. Exceptions for De-Identified (or Anonymized) Data**

We remain concerned that FTC’s breach notification provisions will not apply to data that is de-identified under HIPAA provision 45 CFR 164.514(b).<sup>16</sup> Questions have been raised about whether the de-identification standard (and in particular, the safe harbor method for

---

<sup>14</sup> Section 13400 of ARRA.

<sup>15</sup> Federal Trade Commission, Health Breach Notification Rulemaking, Project No. R911002, Pg. 12.

<sup>16</sup> Id.

meeting that standard) provides sufficient anonymity to data.<sup>17</sup> The privacy risks associated with breached data are context-dependent in that they will be determined by the data analysis tools and other, related sources of data an attacker can use to access and then re-identify breached information. Even if a de-identified data set does not by itself offer enough clues to re-identify patients, the de-identified set can be combined with other data sets that have been stolen or are publicly available. We hope that HHS will use the de-identification study mandated by Congress,<sup>18</sup> as well as its general HIPAA oversight authority, to assess the potential for re-identification of de-identified data and to ensure that entities that disclose or access such data are held accountable for complying with baseline privacy and security protections.

Rather than create a rebuttable presumption that anonymized data sets cannot reasonably be re-identified under any circumstances, FTC should instead rely exclusively on the HHS's "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under the HITECH Act" in determining whether or not data that has been breached is not at risk.<sup>19</sup> We have submitted comments to that Guidance in support of the encryption and destruction standards specified therein and also recommended the addition of a one-way hash function.<sup>20</sup> In our comments, we made the point that whether or not data is identifiable depends on the context (for example, how much data is accessed and how much other data the attacker has or can easily access to re-identify the data) and urged HHS to evaluate technologies and methodologies by means of a threat analysis.<sup>21</sup> Along those lines, we also strongly urged HHS not to add the limited data set to the methodologies that qualify for breach notification exclusion. We likewise urge FTC to acknowledge the contextual nature of identifiability of data and use these same standards and approaches with respect to whether data that has

---

<sup>17</sup> One group of pharmacy researchers tested a set of data de-identified under the safe-harbor method for potential for re-identification. Because the de-identified data contained many unique combination opportunities, the researchers determined that "anticipated [data] recipients, such as physicians, nursing agencies, pharmacies, employers, and insurers...could re-identify their members in the study data set with a moderately high expectation of accuracy." Clause, Steven L., et al, "Conforming to HIPAA Regulations and Compilation of Research Data, *American Journal of Health System Pharmacy*, (61) (2004), 1025-1031, at 1029. See also Bradley Malin and Latanya Sweeney, "How (Not) to Protect Genomic Data Privacy in a Distributed Network: Using Trail Re-identification to Evaluate and Design Anonymity Protection Systems," *Journal of Biomedical Informatics* 37 (2004), 179-192; Latanya Sweeney, "Computational disclosure control, a primer on data privacy protection," (2001) available at <http://www.swiss.ai.mit.edu.proxy1.library.jhu.edu/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf>; Virginia de Wolf et al., "Part II: HIPAA and Disclosure Risk Issues," 28 *IRB: Ethics and Human Research* 6-11 (2006).

<sup>18</sup> ARRA Section 13424(c).

<sup>19</sup> Federal Register/Vol. 74, No. 79/April 27, 2009.

<sup>20</sup> NIST has approved five hashing algorithms that make it computationally infeasible to determine the original data inputs from the hashed data alone. See Federal Information Processing Standard (FIPS) 180-3, *Secure Hash Standard*, Pg. iv (October 2008).

<sup>21</sup> Threat profiling or modeling involves an assessment of the various threats to health data that exist in the environment and then rigorously testing potential technologies and methodologies against whether they effectively mitigate those risks. Of note, NIST has used this process to evaluate the effectiveness of safeguards on electronic voting systems. See NIST, *Developing an Analysis of Threats to Voting Systems*, (October 2005), <http://vote.nist.gov/threats/papers.htm>.

been breached poses a risk to individuals and therefore should trigger notification obligations.

### **C. Presumption that Data that is Accessed has been Acquired**

In proposed Section 318(a), “breach of security” is defined as the acquisition of unsecured identifiable health data.<sup>22</sup> The proposed rule creates a presumption that unauthorized persons have “acquired” information if they have access to it. However, health care entities can rebut this presumption with evidence showing that the information could not reasonably have been “acquired.” The determination of whether the evidence rebuts the presumption of acquisition is an internal decision on the part of the entity.<sup>23</sup>

The presumption of “acquisition” where information has been accessed *by an unauthorized party* is appropriate. The presumption errs on the side of caution by requiring entities to notify patients when it is unclear whether unauthorized parties have acquired health data that has been lost or accessed in a breach. However, FTC should reconsider giving entities broad discretion to determine whether acquisition could have reasonably taken place. The term “acquisition” is undefined in both the ARRA statutory language and in FTC’s proposed rule. ARRA appears to use the term inconsistently in its breach notification provisions, and it is unclear what purpose the distinction between access and acquisition serves.<sup>24</sup>

FTC makes reasonable distinctions between access and acquisition in three scenarios described in the NPRM,<sup>25</sup> but the difference may be extraordinarily difficult to prove accurately and consistently. For example, we agree that scenario (2) qualifies as a data breach but it is unclear how, in this context, acquisition takes place if an employee does nothing more than improperly access the health record of his or her friend. FTC does not explain how to objectively answer this question, but notes there are likely to be other cases in which it is uncertain whether data has been acquired.<sup>26</sup>

However, in its proposed rule, FTC may inadvertently delegate this ambiguity to health care entities to resolve internally. The evidence that health care entities may use to determine whether acquisition occurs is likewise ambiguous. FTC lists some examples of such evidence,<sup>27</sup> but leaves the list open-ended, affording broad discretion to entities in how they make the determination. Computer forensics is perhaps the most objective of the listed evidentiary methods, but acquisition is very difficult to prove or disprove with computer forensics. To do so with forensics, often entities must have imaged the data just before it

---

<sup>22</sup> See also ARRA Section 13407(f)(1).

<sup>23</sup> The entity must demonstrate the evidence to FTC if questioned.

<sup>24</sup> Compare ARRA Section 13407(f)(1) with Sections 13407(b) and 13400(1)(A).

<sup>25</sup> Federal Trade Commission, Health Breach Notification Rulemaking, Project No. R911002, Pg. 8-9.

<sup>26</sup> *Id.*, Pg. 8.

<sup>27</sup> Specifically, “conducting appropriate interviews of employees, contractors, or other third parties; reviewing access logs and sign-in sheets; and/or examining forensic evidence.”

was acquired, in order to compare the state of the data before and after acquisition, but very few entities are able to do this reliably.

The ambiguity of proving whether acquisition occurs compounds the risk that some entities may resolve the issue in a way that is less protective of consumers. While it may be true that health care entities are in a better position to evaluate whether acquisition occurs, those entities also have incentives (both financial and reputational) to avoid having to notify individuals and the government about a breach. Without objective authority or criteria to guide entities' determinations, FTC leaves a large loophole. This would further imply that a determination will only be objectively verified if FTC further investigates whether or not a breach has occurred, which may not be practical for several reasons. Even if it were possible to implement, such an investigation, if it occurs at all, could take place months after the initial breach; if it turns out that the information in fact has been or may have been acquired, individuals are deprived of timely notice that their data is or may be at risk, and the delay in notification decreases their ability to mitigate any damage.

In lieu of a rebuttable presumption, FTC should instead establish a presumption that is not rebuttable that any unsecured PHR identifiable information that is accessed by an unauthorized party is deemed to be acquired. If the entity breaching the data believes there is a chance that the data was in fact not acquired, the entity should include this in the notice to the individual.

#### **D. Meaningful Individual Authorization**

The focus on individual authorization in the definition of "breach of security" in proposed Section 318(a) is consistent with the definition of breach in ARRA. However, we urge FTC to clarify parameters regarding how individual authorization will be determined to give more meaning to this provision. Since individual authorization is central to determining when breach occurs, it is critical that entities offering PHR services obtain authorizations that are meaningful, and informed. The approach described in the Connecting for Health Common Framework for Networked Personal Health Information is that consumers should have meaningful choices spelled out in an understandable way. Consent mechanisms used to obtain a consumer's initial consent should set forth all collections, uses, and disclosures—including the reasons for such uses and disclosures.<sup>28</sup> Entities should obtain the consumer's agreement prior to any collection, use, or disclosure of personal data. Data collections, uses, or disclosures of personal information that could be particularly sensitive or unexpected by a reasonable consumer, should be subject to additional consent and permissions (i.e., independent consent beyond the standard terms of service agreed to upon initiating service), which should be obtained from users in advance of the use or

---

<sup>28</sup> FTC may want to clarify that some access to PHRs, such as for routine account maintenance, are nested within general authorizations; at the same time, any clarification in this regard should not invite vendors and related entities to deliberately use broadly worded or blanket authorizations to avoid triggering notification requirements.

disclosure.<sup>29</sup> Patient authorizations should also be amendable, revocable and proportional to reasonable consumer expectations. Although HHS and FTC will have future opportunities to recommend protections for PHRs in the study required under ARRA,<sup>30</sup> we urge FTC to set these parameters in the breach notification regulations to ensure effective implementation of the breach notification provisions.

## **E. Protecting Data in Motion and at Rest**

FTC should clarify the language in proposed Section 318.2 paragraph (a) defining breach as unsecured information “in a PHR.” Although it is somewhat ambiguous, we believe Congress intended for the breach notification provisions to cover health data at rest (in a PHR or in the hands of a PHR related entity), as well as in transit. This interpretation is endorsed by HHS Guidance, which sets the standards for “unsecured technology” for breach notification of covered entities and PHR vendors. This guidance specifies technologies and methodologies for protecting data both at rest, and in motion, as well as when it is intended to be destroyed.

## **4. Breach Notification Requirements**

### **A. When Breaches are Treated as Discovered**

In the NPRM, FTC notes that it expects PHR vendors and related entities to “maintain reasonable security measures, including breach detection measures, which should assist them in discovering breaches in a timely manner.” Entities that fail to maintain such measures and therefore fail to technically discover a breach will be in violation of the proposed rule because the entity reasonably should have known about the breach. We support this interpretation of ARRA’s provisions on breach discovery, as well as the Commission’s recognition that some breaches may be difficult to detect even with strong security measures. FTC includes a number of suggested resources for “reasonable security measures;”<sup>31</sup> we recommend that FTC add NIST SP 800-66 to this list, which provides recommendations for security protections for data protected by HIPAA.

### **B. Content of Notification**

Section 13402(f) of ARRA (incorporated into Section 13407 of ARRA pursuant to subsection (c)) states that the breach notice provided to individuals must include “a brief description of

---

<sup>29</sup> Markle Foundation, *Consumer Consent to Collections, Uses, and Disclosures of Information Common Framework*, Connecting for Health Common Framework for Networked Personal Health Information (June 2008), <http://www.connectingforhealth.org/phti/reports/cp3.html>.

<sup>30</sup> ARRA Section 13424.

<sup>31</sup> Federal Trade Commission, Health Breach Notification Rulemaking, Project No. R911002, Pg. 18, footnote 12

what happened, including the date of the breach and the date of the discovery of the breach, if known.”<sup>32</sup> In its proposed rule Section 318.6, the Commission interprets this statutory provision to require that the notice to individuals include “a brief description of *how the breach occurred*,” including the date of the breach and date of discovery (if known).<sup>33</sup> We urge FTC to re-establish the original language of the statute and not to expressly require a more detailed description of how the breach actually occurred, as that could inadvertently provide a roadmap for future breaches (both with respect to the initial breaching entity as well as others). Consumers and patients have the right to receive a general description of what happened (which is the language of the statute); providing more detail unnecessarily creates security risks.

## **5. PHR Vendors & Related Entities—Clarifying Which Entity Will Notify Consumers**

Proposed paragraph 318(a) requires PHR vendors and PHR-related entities to provide notification to patients in the event of a breach. Since the legal obligation to notify patients falls to both, it is unclear how vendors and related entities will work out who must notify, especially for situations in which it is unclear who caused the breach. FTC should require a provision in the contracts between vendors and related entities to include a provision establishing which party has the ultimate duty to notify patients in the event of a breach. We believe this duty should fall to the entity that is “closest to the consumer” in cases where it is unclear who is responsible for the breach.<sup>34</sup>

At a minimum, entities should be required to notify each other in the event of a breach. In most instances, this may be the platform on which the PHR is offered rather than a PHR application, but the entities should work together to provide the patient with a single notice with sufficient information, rather than duplicate notices from each entity.

## **6. Enhancing the Effectiveness of Media Notice**

To better reflect changing media consumption patterns, FTC should expand its media notice requirements for breaches of unsecured PHI. Ideally, notice of a breach should appear not just in traditional print or broadcast media, nor simply on a website belonging to the entity or to the government, but also in major Internet media and news outlets. As audiences for traditional media continue to decline, and as traditional media continues to migrate to the Internet, limiting notification to traditional, pre-Internet outlets will have the consequence of reaching fewer and fewer individuals in the event of a breach. Moreover, posting breach notification to websites operated by HHS, FTC or a health care entity is not the equivalent of carrying the notification in websites devoted to delivering news.

---

<sup>32</sup> Section 13402(f)(1) of ARRA.

<sup>33</sup> Emphasis added.

<sup>34</sup> Note that this is distinct from the matter of which entity pays for notification.

In terms of sheer viewership, the Internet news has surpassed all other media outlets except television.<sup>35</sup> Approximately half of Americans turn to the Internet as their top news source, and more Americans identify websites as important and more trustworthy news sources than any other news outlet.<sup>36</sup> Audience age plays a major factor as well; Americans under 30 turn to the Internet in the same numbers as television as their primary news source, and only 7% of Americans under 30 get most of their news from newspapers. Print, television, and radio are increasingly moving to an online format as the trend towards media convergence continues.

Section 13402(e) of ARRA requires a covered entity to notify major print or broadcast media, or to place notice on an entity's website, for breaches of 10 or more individuals for which there is insufficient contact information. The same section requires covered entities to give notice to "prominent media outlets" within the state or jurisdiction of breaches reasonably believed to affect 500 or more residents of that jurisdiction. We believe the language in both contexts is broad enough to encompass these paradigm shifts. "Broadcast media" need not be read to be limited to traditional radio and news outlets, and the term "broadcast" encompasses making information known over a wide area.<sup>37</sup> The term "prominent media outlets" in the post-Internet age surely must be read to include Internet media. We urge FTC to clarify this in the final regulations.

## **7. Clarifying Requirements for Notice to Regulators**

Proposed paragraph (c) requires PHR vendors and related entities to provide notice to FTC no later than five business days after a breach of unsecured PHR information of 500 or more individuals. FTC should clarify whether the clock begins after the breach itself is discovered or after the breach is discovered to affect 500 or more individuals. We recommend that the clock begin once the number of records involved in the breach hits the 500 record threshold. FTC should also make clear that once this threshold is reached, the entity breaching the data must continue to update the Commission regarding the number of records involved in the breach if it grows materially beyond the number initially reported to the Commission.

FTC should clarify that breaches that occur due to the same event or technical vulnerability constitute a single breach event for purposes of determining whether the 500 record threshold is reached (to avoid inviting some entities to define a breach of each record as a separate event in order to avoid hitting the 500 threshold).

---

<sup>35</sup> Pew Research Center for the People & the Press, *Internet Overtakes Newspapers as News Outlet*, (Dec. 23, 2008), <http://people-press.org/report/479/internet-overtakes-newspapers-as-news-outlet>

<sup>36</sup> Zogby International, *Zogby Poll: 67% View Traditional Journalism as "Out of Touch,"* (Feb. 27, 2008) <http://www.zogby.com/news/ReadNews.cfm?ID=1454>.

<sup>37</sup> American Heritage Dictionary, 3d Edition (1994).

Proposed paragraph (c) also states that entities must submit an annual log to FTC for breaches involving fewer than 500 individuals one year from the date of the entity's first breach. FTC should clarify whether that yearly deadline applies to each year after the breach, or whether the clock is reset if the entity does not experience breaches and no log is required.

## **8. State Breach Conflicts**

In its notice of proposed rulemaking, FTC invited information about possible conflicts between the ARRA breach notification provisions and the breach notification requirements in state laws.<sup>38</sup> At least 44 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands have data breach notification requirements.<sup>39</sup> To the best of our knowledge, three states (Arkansas, California and Delaware) have laws that expressly apply to health data. However, it is not readily apparent to what extent other states' breach notification laws would apply to PHRs. There is insufficient time to review the provisions of these laws to appropriately address specific questions in collaboration with HHS, and we hope the agency will not draw any specific conclusions or modify its proposed approach to implementing the breach notification provisions based on blanket statements about possible conflicts or speculation that individuals might be subject to receiving multiple notices.

However, we recognize the possibility that there could be issues that need to be resolved, and we suggest that FTC and HHS work with Congress to call for a study—perhaps by the Government Accountability Office or the Congressional Research Service—to review state breach notification laws and address the questions raised by FTC and HHS. The agencies will then have objective data upon which to base its decisions, or to use to approach Congress if the agency thinks statutory changes are needed.

## **9. It is Reasonable for FTC to Determine that the Temporary Breach Notification Provisions Are an Expansion of its Section 5 Authority**

As a final note, FTC's conclusion that Section 13407 of ARRA expands the scope of FTC's enforcement jurisdiction beyond the entities over which it has traditionally had authority, to include nonprofit entities, is reasonable. As a threshold matter, Section 13407 was enacted as a separate grant of temporary authority to the FTC over PHR vendors (which are defined in ARRA) and PHR related entities (described in Section 13424(c) of ARRA). The sole reference to the FTC Act is the incorporation by reference of the penalty provisions of a regulation under Section 18(a)(1)(B) of the FTC Act. Specifically, Section 13407(e) of ARRA states that violations of the breach notification provisions "*shall be treated as* an unfair and

---

<sup>38</sup> Federal Trade Commission, Health Breach Notification Rulemaking, Project No. R911002, Pg. 40.

<sup>39</sup> National Conference of State Legislatures, State Breach Notification Laws, (Dec. 16, 2008), <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

deceptive act or practice” in violation of the FTC Act.<sup>40</sup> Such language indicates Congress’ intent to have failures to notify in the event of a breach “treated” the same as an unfair and deceptive act or practice would be under the FTC Act.

Of note, Congress recently used similar language to incorporate FTC Act penalties in a statute that also broadened the FTC’s traditional jurisdiction. In the Sports Agent Responsibility and Trust Act,<sup>41</sup> Congress places clear rules on “athlete agents” with respect to their contacts with student athletes. The term “athlete agent” is specifically defined in the Act. Violations of the Act are “treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the [FTC Act].”<sup>42</sup> There is no plausible argument that FTC’s authority to enforce this statute is limited to those “athlete agents” who are already covered by the FTC’s Section 5 jurisdiction.

For an example of Congress acting to confine FTC’s jurisdiction to its traditional Section 5 authority, see the Telemarketing and Consumer Fraud and Abuse Prevention Act.<sup>43</sup> In this Act, Congress provides that “this chapter shall be enforced by the Commission under the Federal Trade Commission Act. Consequently, *no activity which is outside the jurisdiction of that Act shall be affected by this chapter.*”<sup>44</sup>

## **10. Conclusion**

We appreciate the opportunity to provide these comments in response to FTC’s notice of proposed rulemaking on the ARRA breach notification provisions that apply to PHR vendors and PHR-related entities. In summary, we suggest FTC:

- Work with HHS to apply consistent information and breach policies to PHRs in order to provide consumers with a reliable framework of protections;
- Ensure that individuals acting in a personal capacity are not considered to be a PHR related entity;
- Maintain its interpretation of the types of data that constitute PHR identifiable information;
- With respect to whether or not data is “identifiable,” rely on HHS’ Guidance<sup>45</sup> in determining whether or not data that has been breached is not at risk and acknowledge that the question of identifiability depends on the context;

---

<sup>40</sup> Emphasis added.

<sup>41</sup> P.L. 108-304, 118 Stat. 1125 (codified at 15 USC 7801 et al.)

<sup>42</sup> 15 USC 7803(a).

<sup>43</sup> Codified at 15 USC 6101-6108.

<sup>44</sup> 15 USC 6105(a) (emphasis added).

<sup>45</sup> “Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under the HITECH Act”

- Presume that unsecured PHR identifiable information that is accessed by an unauthorized party is deemed to be “acquired”;
- Ensure the breach definition is meaningful to individuals by setting parameters for authorization;
- Protect data in motion as well as at rest (and not just “in the PHR”);
- Add NIST SP 800-66 to the list of potential resources for reasonable security measures;
- With respect to the content of the notice to individuals, adhere to the statutory language and avoid imposing content requirements that could be a roadmap to lead to future breaches;
- Clarify which entities are accountable for notifying consumers in the event of breaches that may involve multiple parties;
- Revise the media notice requirements to specifically incorporate new media;
- Clarify timing issues with respect to notice to the FTC of breaches; and
- Support a study of state breach notification provisions to determine whether the new federal provisions conflict with existing state law, and whether state and federal laws will result in individuals receiving duplicate notices.

FTC’s conclusion that the temporary breach notification provisions in Section 13407 of ARRA apply to all PHR vendors and PHR related entities and not just those that are also covered by the FTC’s authority under Section 5 of the FTC Act is also appropriate.

Please let us know if you have any questions or need further information.

Sincerely,

Center for Democracy & Technology  
Markle Foundation  
Childbirth Connection  
Health Care for All  
National Partnership for Women & Families  
SEIU