RIN 0991-AB56

HITECH Breach Notification for Unsecured Protected Health Information Rulemaking

October 23, 2009

Georgina Verdugo, Director
Office for Civil Rights
United States Department of Health and Human Services

Dear Ms. Verdugo:

The Markle 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, while protecting privacy. 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. Markle, and CDT, along with those listed at the end of this letter, submit these comments in response to the interim final rule (IFR) establishing requirements for notification of breaches of unsecured protected health information and request for comments issued by the Department of Health and Human Services (HHS) under the American Recovery and Reinvestment Act of 2009 (ARRA).[1]

The HHS IFR, which applies to entities covered by the Privacy and Security Rules of the Health Information Portability and Accountability Act (HIPAA), was issued at around the same time the Federal Trade Commission (FTC) issued its final rule[2] governing breach notification for personal health record (PHR) vendors and related entities that are not HIPAA-covered entities (collectively referred to as PHR vendors).[3] Because there is overlap between these two sets of standards, we have taken the FTC's final rule into account in formulating these comments on HHS' IFR. We also address HHS' clarification of guidance, issued contemporaneously with its IFR, which specifies the secure technologies and methodologies that when utilized by HIPAA-covered entities or PHR vendors provide a safe harbor from the ARRA's breach notification requirements.

---

[1] HHS, Breach Notification for Unsecured Protected Health Information; Interim Final Rule, Federal Register, Vol. 74, No. 163, pp. 42740 – 42770, August 24, 2009 (HHS IFR or IFR).

[2] FTC, Health Breach Notification Final Rule, Federal Register, Vol. 74, No.163, pp. 42962 – 42984, August 25, 2009 (FTC Final Rule).

[3] The FTC rule requires ''vendors of personal health records'' and ''PHR related entities, to notify their customers of any breach of unsecured, individually identifiable health information. ARRA expressly excludes from the definition of "vendors of personal health records" entities covered by the HIPAA Privacy Rule. American Recovery and Reinvestment Act of 2009, P.L. 111-5 (ARRA), § 13400(3) and (18).

Our comments are based on a few core principles:

- A comprehensive framework of privacy protections, including greater transparency regarding uses and disclosures of personal health data, is crucial to consumer trust in health information technology and health information exchange.
- Requiring that individuals and government authorities be notified in the event of a breach of personal health information promotes transparency and acknowledges concerns that individuals have when their health data are inappropriately accessed or disclosed. Breach notification requirements are part of a strategy to help health care organizations develop and implement policies and technologies that better protect health data.
- Policies and standards for breach notification should be set in a way that promotes these important goals while also avoiding over-notification for inconsequential breaches.
- It is essential to have a consistent and consumer-oriented approach to privacy and security policies for personal health records or systems (PHRs) in order to avoid confusing and potentially harmful policies for this emerging set of tools for enabling consumers to manage and use their health information to improve their care.

I. Overview

As noted above, it is critical that policies for notification in the event of a breach of health data be set in a way that accomplishes the purposes of breach notification while also not overly burdening industry and consumers with notification when the breach is inconsequential. We have identified a number of areas where the IFR policies raise concern:

- Under the IFR, a covered entity need only notify individuals when an inappropriate use or disclosure of protected health information "poses a significant risk of financial, reputational, or other harm to the individual." The IFR delegates to the covered entity the decision as to whether there is significant risk of harm to the individual without any clear, objective criteria on how risk of harm is to be assessed. Such an open-ended approach to notification will be more burdensome to industry because it will require each entity to determine what standard of harm it will use. It will also be more burdensome to OCR to make judgment calls based on subjective, individualized assessments, and burdensome to consumers who will not know how each entity is individually assessing harm. Imposing additional burdens on industry in the absence of evidence that this approach is the best for advancing the policy goals of breach notification seems particularly unwise in a time of enormous challenge for the health care industry given all of the new obligations that will come from ARRA. We suggest in these comments an alternative, objective approach that can be more consistently applied and enforced.

- There are other aspects of the IFR that merit further consideration:
    - Creating a safe harbor for inappropriate uses and disclosures of certain partially de-identified information (limited data sets minus dates of birth and zip codes) by deeming release of this data not to compromise the security or privacy of the protected health information is not advisable in the absence of an assessment of the recipient's potential ability to re-identify the information.
    - Allowing information unintentionally accessed or acquired by an employee to be further used or disclosed in any manner permitted under the Privacy Rule, which includes a wide variety of treatment, payment, and health care operations purposes, is also not advisable. The IFR should require mitigation of further use or disclosure even if the unintentional access is immediately discovered.
    - Finally in the area of Personal Health Records, there is a need to carefully reexamine the potential consequences of having different policies for individuals whose health data are part of a personal health record offered by a covered entity versus a non-covered entity.

In sum, we ask HHS to:

- Revise the individual harm standard that HHS added as a trigger to the breach notification requirement, by deleting 45 C.F.R. § 164.402(1)(i) and replacing it with objective standards for judging whether the data have been "compromised" that can help entities determine whether the data are at significant risk of being inappropriately viewed, re-identified, re-disclosed, or otherwise misused.
- Issue annual or at least periodic guidance on best risk assessment practices for breach notification.
- Recognize that the potential re-identification risk of limited data sets, even when dates of birth and zip codes have been removed, is dependent on the receiver; determine that this information should not, as a standard matter, be given safe harbor status without any risk assessment; and eliminate or strengthen 45 C.F.R § 164.402(1)(ii) in the final version of the breach notification rule to include an assessment of risk with a high burden of proof.
- Require workforce members of covered entities who discover that they have inadvertently accessed or received information to take appropriate steps to mitigate against further use or disclosure of such information.
- Ensure PHRs will have consistent and consumer-oriented privacy and security protections for PHRs by clarifying that, with respect to a PHR offered by a covered entity or a business associate and marketed as giving consumers control over their health information, the breach definition language "unauthorized acquisition, use or disclosure," means acquisition, use or disclosure of protected health information without the permission of the individual. Such an interpretation would bring HHS'

breach notification rule in better alignment with the FTC's breach notification requirements.

- Amend the Privacy Rule so that the privacy notice of any covered entity with a PHR must clearly state the covered entity's use and disclosure of information in the PHR (as opposed to permitted uses and disclosures), and require the covered entity to abide by the terms of its notice.

II. Setting Clear Parameters for When Notification Must Occur

A. Whether health information has been compromised should be determined by an assessment of the risk that the data were inappropriately viewed or used or could be re-identified.

We recognize the potential for unnecessary notifications if patients are contacted for each and every inconsequential breach. We also recognize that some technical breaches (e.g., a health care provider sending a prescription to the wrong pharmacy) may indeed pose risks that are so insignificant that notification would not be meaningful in those instances.

With respect to the duty of covered entities to notify patients of data breaches, the ARRA generally defines "breach" as the "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information."[4] Under HHS' interpretation in the IFR, breach does not occur unless the access, use or disclosure poses "a significant risk of financial, reputational, or other harm to the individual."[5]

Our concern about this interpretation is that it doesn't provide any objective criteria for evaluating whether a particular breach should result in notification to an individual and to HHS. Instead, it focuses narrowly on whether there has been "financial, reputational or other harm" to the individual who is the subject of the data, which will be difficult if not impossible for entities to determine with any degree of confidence.

The statutory term "compromises the security or privacy of data" invites HHS to set an objective standard for breach notification, which ensures that the purposes for requiring breach notification are met while also minimizing the burdens that could result from over-notification. Instead of the current interpretation, we suggest that HHS require entities to do a risk assessment to determine whether or not the data involved in the breach were at significant risk of being inappropriately viewed, re-identified, re-disclosed, or otherwise misused.

HHS already indicates in the preamble to the IFR that an entity that has discovered a security or privacy breach should be required to undertake an investigation and an

---

[4] ARRA, § 13400(1)(A).

[5] 45 CFR §164.402; HHS IFR at 74 Fed. Reg. 42767.

assessment to determine whether the data were at risk.[6] We suggest using a risk-based standard for assessing whether or not data were "compromised" that would require covered entities to consider the following four areas:

1. to whom the information was impermissibly disclosed;
2. whether the information was actually accessed or viewed;
3. the potential ability of the recipient to identify the subjects of the data; and
4. in cases where the recipient is the disclosing covered entity's business associate or is another covered entity, whether the recipient took appropriate mitigating action.[7]

These factors should not be considered in isolation, nor is satisfying one factor necessarily sufficient. For instance, it would be necessary to consider the risk of identification in the context of who received the information, what motivation they had to identify the information, and what other information they had access to. Whether the individual may be demonstrably harmed or is capable of remedying the loss of his or her data should not factor into the assessment. Entities should be required to document and keep a record of their determination that an incident has not compromised the privacy and security of the information involved as assessed against each of these four areas of the risk standard.

For purposes of this assessment, appropriate mitigation should be considered the prompt destruction of the inappropriately received information in accordance with HHS guidance on secure technologies and methodologies or the prompt return of the information, without further use or disclosure of the information.

For example, a doctor's office may send a prescription to the wrong pharmacy. The pharmacy notices the error, notifies the doctor's office, deletes the information from its system and informs the doctor's office of its action. In making an assessment of whether notification was required, a covered entity would consider the fact that the information was impermissibly disclosed to another covered entity, and that even though the information was viewed in identifiable form, the covered entity receiving the information had promptly taken mitigating steps to prevent further disclosure. In this case it would appear that the information has not been compromised and that notification would not be necessary.[8] If the covered entity has insufficient information to determine whether the data were put at risk, the presumption should be that a breach has occurred and notice is required.

---

[6] The assessment requirement, of course, does not apply to data encrypted or destroyed according to the standards established in the HHS guidance.

[7] HHS discusses this factor in the IFR where it points out that there may be less risk when the breached information was received by covered entities that are under the same obligations to protect the privacy and security of the information as the entity that disclosed the information. The proposed assessment of risk to data is a means of ensuring that covered entities fulfill those obligations before they may avoid patient notification. See HHS IFR at 74 Fed. Reg. 42744.

[8] We note that ARRA specifically permits an individual to direct health care providers to withhold certain information from health plans when the individual self-pays for treatment. ARRA, § 13405(a). Under those circumstances, the inappropriate disclosure of such information to a health plan should be deemed to compromise the privacy and security of data.

This *de minimus* risk standard preserves the goals of data protection, transparency and consumer education, while avoiding unnecessary notifications. This approach is also more consistent with the standard used in the Federal Trade Commission's (FTC) breach notification rule, which requires notification based on whether the information was actually viewed, as opposed to the recipient's merely having the opportunity to view the information.[9] We also believe that this standard is more consistent with the statutory language, which defines breach as exposure that compromises the privacy or security of the information – and not the finances or reputation or other tangible interest of the patient. As we set forth in more detail below, the focus on individual harm injects too much subjectivity into what should be an objectively applied standard and risks overly burdening industry, who will have to develop their own harm assessments in the face of uncertainty regarding whether or not HHS will agree with their validity. It also burdens HHS, who will be held accountable for judging these individualized standards and also educating the public, in order to fulfill transparency and oversight goals, on the various approaches being used by industry to comply with the statute. Consumers also will not know how different covered entities are assessing harm.

We urge HHS to revise its current breach notification standard and adopt the risk assessment standard we have outlined in these comments to reduce unnecessary breach notifications while implementing the statute in a way that promotes consistency and objectivity and earns patient trust. Enforcement of the standard is not due for another 120 days,[10] and it would be beneficial to revise the standard while it is still new, before it is institutionalized throughout the health care system.[11]

We have set forth some objective criteria for covered entities to use in determining whether or not data involved in a breach are at risk. Industry and consumers could benefit from increased transparency about how such risk assessments are made and best practices for making them. HHS could ask covered entities to include in their Notice of Privacy Practices the internal policies they use in determining whether or not a breach will trigger notification. We also encourage HHS to issue a request for information to obtain similar, commonly recurring incidents so that it can issue more detailed guidance on when information would be considered to be at risk.

Finally, strong oversight is required to ensure that covered entities base their risk assessments on appropriate factors. To this end, we urge HHS to audit and evaluate the documentation of such determinations when carrying out the compliance audits required by the ARRA. To the extent any pattern of misunderstanding or misuse of these criteria becomes evident, HHS should issue further clarifying guidance.

---

[9] FTC Final Rule, 74 Fed. Reg. at 42966.

[10] HHS IFR at 74 Fed. Reg. 42757.

[11] Further, it is fair for HHS to consider revisions to this standard, given that there was no public comment period prior to publication in the IFR.

B. Concerns about a standard that rests on harm to the individual

We are concerned about the subjectivity implied by the current harm standard in the IFR. HHS indicates in its IFR that that covered entities should consider the nature of the protected health information in making a risk assessment.[12] HHS suggests that merely disclosing the name of an individual and the fact that he received services from a hospital may not constitute a risk of financial or reputational harm to the individual, despite violating the Privacy Rule.[13] However, the covered entity is not in a position to be able to adequately assess whether such information would harm an individual. There are countless examples in which this same information may cause harm if not kept discreet: for instance, the information could damage an executive's chances for promotion or place domestic abuse victims at risk.

In addition, we place value on the privacy and security of health information even if no significant harm can be shown to individuals. Improper employee access of health information of friends, neighbors, and well-known people is a violation of health information privacy and security that occurs frequently. Yet, it may not be possible to pinpoint a specific or substantial harm to the person whose information has been improperly accessed.

The likelihood that individual circumstances will be carefully considered in every case is remote. It must be kept in mind that the "significant risk of harm" determination is an internal process on the part of companies who could have a financial and reputational bias against notification. Even industry representatives recognize the potential for abuse. In a recent trade publication, the information technology security manager of a 400-bed medical center acknowledged harm was "in the eye of the beholder" and that under the rule "a covered entity is now strongly incentivized not to report and now has the cover – the harm threshold – to support that decision in any but the most obvious case."[14]

HHS further justifies its approach as providing better alignment with state breach notification laws.[15] However, HHS acknowledges in its IFR that state laws vary significantly.[16] Entities are required to comply with state breach notification laws if those laws are stricter than the notification requirements promulgated by HHS. Several states' laws do not include an individual harm standard as the trigger for breach notification, instead requiring such notification if protected data are "acquired". Among these states are four of the five most populous: California,[17] Illinois,[18] New York[19] and Texas.[20] Combined,

---

[12] HHS IFR at 74 Fed. Reg. 42745.

[13] HHS IFR at 74 Fed. Reg. 42745.

[14] " 'Harm' Standard May Mean Fewer Breach Notices, but More Complications for CEs." Report on Patient Privacy, Volume 9, Number 10, October 2009, Pg. 3. A just released Ponemon Institute study found that 80 percent of healthcare organizations surveyed had experienced at least one incident of lost or stolen electronic health information in the past year, and four percent had more than five patient data breaches. http://www.loglogic.com/resources/analyst-reports/ponemon-electronic-health-info-at-risk/.

[15] HHS IFR at 74 Fed. Reg. 42744.

[16] HHS IFR at 74 Fed. Reg. 42758.

[17] Cal. Civ. Code § 1798.82.

[18] 815 Ill. Comp. Stat. § 530/10.

[19] NY Gen. Bus. Law § 899-aa.

[20] Tex. Bus. & Com. Code § 48.103.

these states make up more than thirty percent of the United States population, with California alone comprising more than one-tenth of the population.[21] Any entity doing business with these states or on a nationwide basis must comply with the laws of these states. Given such variation among states, meaningful alignment of breach notification laws has not been achieved by the imposition of the harm standard. We also note that in 2005, the National Association of State Attorneys General sent a letter to Congressional leadership urging them to adopt a federal breach notification standard based on risk to data and not harm to the individual.[22]

Moreover, as HHS notes,[23] state breach notification laws are "generally focused on breaches of financial information rather than on health information".[24] HHS' grafting of a "significant risk of harm to an individual" standard used in the financial services industry onto the health care industry is misplaced. Health data relate to a different subject matter than financial data, with its own set of special sensitivities, and with respect to which different people may have idiosyncratic (or different) privacy preferences.

A better way to address individual harm to patients is to require breaching entities to include their assessment of the risk of individual harm in the notice itself. ARRA already requires breaching entities to include in patient notifications a description of what happened, what information was breached, and what steps patients may take to protect themselves.[25] Breaching entities could also include a conspicuous, concise statement on the notice informing patients of the perceived level of threat posed to the individual. This would prevent unnecessary concern while still enabling patients to take steps to protect themselves if their individual circumstances so warrant.

III. Safe Harbor Status

Section 13402 of the ARRA requires covered entities to notify individuals following the discovery of a breach of unsecured protected health information. Section 13407 of the ARRA imposes similar requirements on PHR vendors when there has been a breach of unsecured PHR identifiable health information. With respect to both of these provisions, "unsecured"

---

[21] United States Census Bureau, National and State Population Estimates 2000 to 2008, http://www.census.gov/popest/states/NST-ann-est.html. We note that the breach provisions in each of these four states apply only to computerized data.

[22] Quoting from the letter: "We also believe that the standard for notification should be tied to whether personal information, whether in electronic or paper form, was, or is reasonably believed to have been acquired or accessed by an unauthorized person, rather than a standard that includes an additional requirement that the breach entail actual harm or a measure of risk of harm. Standards that require additional proof by a tie to harm or to a risk of harm place the bar too high. It is extremely difficult in most cases for a breached entity to know if personal data that has been acquired from it by an unauthorized person will be used to commit identity theft or other forms of fraud." http://www.cdt.org/security/State_AGs_2005_Letter_to_Congress_on_Breach_Notification.pdf. The letter was signed by Attorneys General from 45 states, the District of Columbia, Puerto Rico, and the Northern Mariana Islands.

[23] HHS IFR at 74 Fed. Reg. 42758.

[24] See, e.g., Ga. Code § 10-1-910 (explaining that prevention of identity theft is the basis for the Georgia breach notification law).

[25] ARRA § 13402(f).

means information that is not secured through the use of a technology or methodology specified by the Secretary in guidance as rendering protected health information unusable, unreadable, or indecipherable to unauthorized individuals.[26] Information that has been protected using the specified technologies or methodologies is not subject to the breach notification requirements, essentially creating a safe harbor.

On April 27, 2009, HHS published its guidance specifying encryption and destruction as the technologies and methodologies meeting this standard. HHS' exhaustive list of the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals include the following:

- For electronic PHI at rest, data that have been encrypted using a process consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, Guide to Storage Technologies for End User Devices.
- For electronic PHI in motion, data that have been encrypted using a process that complies with the requirements of Federal Information Processing Standards (FIPS) 140-2.
- Paper, film or other hard copy media that have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.
- Electronic media that have been cleared, purged or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

HHS solicited public comment on whether it should consider adding additional technologies and methodologies to this list in future iterations of guidance.

A. Encryption

As we noted in our comments to the original guidance, we support the inclusion of the items on this list as being strong, current data encryption and destruction standards.[27] We note that encryption need not be expensive, so the technology is accessible even by providers with limited resources. We continue to recommend the addition of the one-way hash to the list, which is broadly useful for population health analysis to permit linking separate databases without exposing underlying information. We also continue to urge HHS to annually revisit this guidance to ensure that it keeps pace with (and encourages) innovation in data protection technologies and methodologies.

---

[26] ARRA, § 13402(h).

[27] Comments of the Markle Foundation, Center for Democracy & Technology, et al., to 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 American Recovery and Reinvestment Act of 2009, May 21, 2009, http://www.connectingforhealth.org/resources/20090522_breach_methodologies.pdf.

B. Access Controls

We wholeheartedly support HHS' determination in its updated guidance that access controls do not meet the statutory standard. As HHS noted, access controls are important tools for safeguarding protected health information. However, if access controls are compromised, the underlying information may still be usable, readable or decipherable to an unauthorized individual. We laud HHS' approach on this issue. Use of access controls does not warrant the same safe harbor status accorded to encryption.

C. Limited Data Sets

We are concerned about HHS effectively granting safe harbor status to a subset of the limited data set (i.e., a limited data set from which dates of birth and zip code have been removed "LDS Lite") by deeming the inappropriate use or disclosure of such information as not being a breach without an assessment of risk of re-identification.

A limited data set is protected health information which has been partially de-identified by removing most identifiers including the name, address, social security number, and account number of an individual or the individual's relative, employer, or household member.[28] Unlike information that has been de-identified in compliance with HIPAA, a limited data set may include dates (e.g., dates of birth, admission dates, and dates of service) as well as town or city, State, and zip code. Because of the potential for re-identification, limited data sets may be used and disclosed without authorization only for research, public health or heath care operations and only when the recipient has signed a data use agreement. Under such a data use agreement, the recipient must agree, among other things, not to identify the information or to contact the individuals and to use or disclose information only for the limited purposes specified above.

Recognizing the potential risk of re-identification of limited data sets, HHS excluded this means of partially de-identifying information from the list of technologies and methodologies that render information unusable, unreadable, or indecipherable to unauthorized individuals and thus entitled to safe harbor status under section 13402(h) of the ARRA. However, HHS then effectively gave a subset of limited data sets safe harbor status from the breach notification provisions through this IFR. In the IFR, HHS deems the inappropriate use and disclosure of limited data sets from which dates of birth and zip codes have been removed (LDS Lite) to not compromise the security or privacy of protected health information.[29] As a practical matter, this approach creates a safe harbor. Under the IFR, when LDS Lite information is inappropriately used or disclosed, covered entities are never required to notify individuals of such disclosure regardless of the recipient of the information. Neither are covered entities required to conduct a risk analysis to evaluate the recipient's potential ability to re-identify the information. HHS justified this approach on its belief that the

---

[28] The Privacy Rule deems as "de-identified" protected health information from which 18 specified identifiers have been removed. 45 C.F.R. § 164.514(b). A limited data set is created by removing 16 of these 18 identifiers. 45 C.F.R. § 164.514(e)(2).

[29] 45 C.F.R. § 164.402(1)(ii).

inappropriate use and disclosure of LDS Lite if subjected to a risk assessment would pose a low level of risk.[30]

As we noted in our comments to the original guidance on secure technologies, given rapidly evolving technologies and increasing availability of databases, it is not appropriate to deem information to not be at risk solely because it has had specific identifiers removed. It is more appropriate to describe a spectrum of "identifiability," rather than a binary classification of information that may be identifiable or not. The question is not just what identifiers are still present in the data set but also which entities would be able to re-identify the information, how much effort they would have to expend, and what limits are placed on their doing so.[31]

While it may be true that stripping an LDS of zip codes and dates of birth may make it less likely that the information will be re-identified, the level of risk of re-identification also depends on the recipient of the information. The risk of re-identification of data subjects may be small when an average thief with little if no ability or motivation to identify the data subjects steals a laptop with LDS Lite. However, impermissibly releasing information to recipients who have access to other large databases of individually identifiable information heightens the risk that the information in the LDS Lite may be combined with other data and re-identified. One of the few studies conducted on the HIPAA de-identification standard demonstrated that the risk of re-identification of data can be real. The study found that employers, physicians, pharmacies, employers and insurers could identify members by applying diagnosis and medication combinations to a de-identified data set with a moderately high expectation of accuracy.[32] It is quite clear that the risk of re-identification of data in an LDS Lite format depends largely on the recipients of the data, their access to other information, capabilities and motivation.

In sum, information in LDS Lite would not always meet the standard of being unusable, unreadable or indecipherable and therefore should not be given general safe harbor status. It does not qualify as a "secure" technology entitled to safe harbor status under section 13402(h) of ARRA.

Instead whether a covered entity is required to give notice of the inappropriate use or disclosure of information in LDS Lite format should be determined under the risk assessment described above, and in particular by the risk that the information will be compromised by being re-identified in the specific circumstances at hand. We urge HHS to eliminate 45 C.F.R § 164.402(1)(ii) from the final version of the breach notification rule.

---

[30] HHS IFR, 74 Fed. Reg. at 42746.

[31] See Markle Foundation, CT4: Limitations on Identifying Data, Connecting for Health Common Framework for Networked Personal Health Information (June 2008),http://www.connectingforhealth.org/phti/reports/ct4.html.

[32] Steven Clause, et al. "Conforming to HIPAA Regulations and Compilation of Research Data," 61 American Journal of Health System Pharmacy 1025-1031 (2004).

IV. Inadvertent Access or Acquisition

The ARRA excludes from the definition of breach certain cases of unintentional acquisition of protected health information, provided such information is not "further acquired, accessed, used, or disclosed without authorization."[33] The HHS IFR contradicts this statutory framing by allowing the entity inadvertently receiving this information to use it in any way permitted under the Privacy Rule.[34] Under HHS' interpretation, once a covered entity has inappropriately, but unintentionally, accessed information, they may use it in any manner that conforms to the Privacy Rule.

The workforce members of a covered entity should not be able to further use or disclose the information that they improperly accessed just because the improper access was inadvertent. Such a framework opens the door to a wide variety of uses and disclosures, and may undermine the purpose of requiring breach notification.

At a minimum, we urge HHS to limit the breach notification exception for inadvertent disclosures in circumstances where the workforce member knows or should have known that they have accessed or received information that was not intended for them to cases where the workforce member has taken steps to mitigate the improper access or receipt. At the outset we note that this standard complements the duty to mitigate imposed by section 164.530(f) of the Privacy Rule. In addition, this proposed standard conforms to one of HHS' examples of incidental access, which would not be considered a breach under the IFR. For example, a billing employee receives and opens an e-mail containing PHI about a patient which had been misdirected. Upon noticing that he was not the intended recipient of the e-mail, the employee alerts the nurse who sent it and destroys the e-mail. HHS should clarify that this type of mitigating behavior is required of all employees who recognize that they have unintentionally accessed PHI to which they are not entitled in order for the covered entity to qualify for the breach notification exception.

In addition, when a workforce member discovers that he has inappropriately, although inadvertently, shared information with another person, he should be required to notify the recipient of the error and request destruction or return of the information, to the extent practicable. There should not be a simple "free pass" just because the information was unintentionally accessed or shared. This information should not be further disclosed or reused, except to mitigate the initial unintentional exposure.

---

[33] ARRA, § 13400(1)(B).

[34] 45 CFR § 164.402(2)(i) provides that "breach does not include:

Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part."

V. Timing of Notice to Secretary

The IFR's 60-day deadline for reporting breaches to the Secretary is contrary to the "immediate" notice required by the ARRA.[35] Section 13402(d) of the ARRA requires a covered entity to furnish required breach notification to affected individuals without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered. In contrast, Section 13402(e)(3) of the ARRA requires covered entities to notify the Secretary "immediately" of breaches of unsecured protected health information involving 500 or more individuals. Even though this latter provision clearly establishes a different deadline for notifying the Secretary vis-a-vis notifying an affected individual, HHS has interpreted it as having the same meaning -- that covered entities are required to provide notice to the Secretary concurrent with providing notice to the individual. This interpretation is contrary to generally accepted rules of statutory construction that the use of different phrases in a statute have different meanings. Providing notice to the Secretary in advance would allow HHS to provide technical assistance in crafting and furnishing breach notification if appropriate.

VI. Personal Health Records (PHRs)

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 electronically 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. The ARRA addresses PHRs and recognizes their consumer-centeredness by defining a personal health record as: an electronic record of PHR identifiable information[36] . . . on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.[37]

Some entities offering PHRs are subject to the existing privacy and security requirements of HIPAA. These entities are governed by the breach notification provisions for HIPAA-covered entities.[38] With respect to PHRs offered by entities not covered by HIPAA, the ARRA requires HHS to study, in consultation with the FTC, potential privacy, security, and breach notification requirements and to submit a report to Congress containing recommendations

---

[35] Of course, we note that the entity will need time to perform its risk assessment and determine whether or not notification is required.

[36] ARRA, § 13407(f)(2) defines PHR identifiable information as individually identifiable information as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes with respect to an individual, information— (A) that is provided by or on behalf of the individual; and (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

[37] ARRA, § 13400(11) (emphasis added).

[38] See ARRA, § 13400(18) defining vendor of personal health records as excluding entities covered under HIPAA. The FTC Final Rule also makes clear that PHRs offered by covered entities are subject to HHS breach notification rules. FTC Final Rule at 42963.

within one year of enactment of the Act. Until Congress enacts new legislation implementing such recommendations, the ARRA contains temporary requirements, to be enforced by the FTC, that such non-HIPAA covered entities notify individuals in the event of a breach of unsecured PHR identifiable health information.[39]

Several of the ARRA's provisions that govern HIPAA-covered entities also apply to non-HIPAA covered entities. Due to this overlap, HHS and the FTC consulted with each other in order to "harmonize" their rules.[40] Unfortunately, notwithstanding efforts to harmonize, the breach notification rules issued by HHS and FTC differ significantly, with important consequences for consumers. As discussed in more detail below, we urge HHS to align its breach notification rule with that issued by the FTC, which is more transparent and consumer-oriented.

In June 2008, Markle Connecting for Health released the Common Framework for Networked Health Information[41] outlining a uniform set of meaningful privacy and security policies that are appropriate for all entities that may provide consumers with personal health records (which may include copies of health data generated by a covered entity as well as data the individual inputs him or herself). This framework — which was developed and supported by a diverse and broad group of more than 55 organizations including technology companies, consumer organizations and entities covered by HIPAA[42] — was designed to meet the dual challenges of making personal health information more readily available to consumers, while also protecting it from unfair or harmful practices. The framework is based on the principle that personal health records and other consumer access services are tools for consumers' use, and are controlled and managed by consumers.[43] PHRs are marketed by many entities (both HIPAA-covered and others) as a means for consumers to control their health information. This paradigm has two central policy implications: 1) That a consistent and consumer-oriented set of rules apply to PHRs regardless of the entity offering them; and 2) That the consumer's preferences with respect to sharing the copy of information in their PHR be recognized and implemented.

The HHS IFR potentially contradicts (or conflicts with) both of these policy goals. The FTC final rule requires non-HIPAA covered entities to furnish notification when there has been an acquisition of PHR identifiable information without the authorization of the individual.[44] Under the HHS IFR, in contrast, covered entities that offer PHRs are required to notify the individual only if the information in the PHR is used or disclosed in a manner not authorized by the HIPAA Privacy Rule. In such a case the individual's preferences become largely irrelevant, which is particularly problematic when the information at issue has been

---

[39] ARRA, § 13407(a).

[40] FTC Final Rule; HHS IFR.

[41] See http://www.connectingforhealth.org/phti/#guide.

[42] See list of endorsers of the Markle Connecting for Health Common Framework for Networked Personal Health Information at: http://www.connectingforhealth.org/resources/CCEndorser.pdf.

[43] 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.

[44] 16 C.F.R. § 318.2.

voluntarily entered by the consumer into a PHR that has been marketed as being "consumer controlled". The IFR also varies from FTC's final breach notification rule for PHR vendors in several other significant ways. The result is that consumers will be subject to varying degrees of protection depending on what type of entity offers the PHR service, a distinction that the consumer will have a hard time making for seemingly identical offerings. It is 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, a distinction consumers should not be expected to make easily.

We urge HHS to amend the interim final rule to reflect a more consumer-oriented and consistent approach. Specifically, we urge HHS to clarify that, with respect to a PHR offered by a covered entity or a business associate and marketed as giving consumers control over their health information, the breach definition language "unauthorized acquisition, use or disclosure," means acquisition, use or disclosure of protected health information without the permission 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."[45] It is also consistent with the FTC's breach notification standard.

This standard would apply to products marketed as a means for consumers to control, manage and share their health information. We recognize that some services offered by covered entities that are commonly called PHRs do not permit consumers to enter their own information or do not purport to offer consumer control. These services are really just portals into the covered entity's own operational record (e.g., their legal medical record). Since consumer expectations are different with respect to a covered entity's operational record, HHS' interpretation of "unauthorized" as meaning in violation of the HIPAA Privacy Rule makes sense with respect to this type of record.

On a broader scale, we also encourage HHS to revisit the requirements of the Privacy Rule in light of changes in the marketplace that have occurred since the Rule was last revised in 2002. PHRs are becoming more prevalent and are offered by more organizations, including covered entities. We believe that the Privacy Rule should reflect these changes and should incorporate the consensus principles for PHRs detailed in the Common Framework. In particular, the Privacy Rule should be revised to require covered entities to include in their notice of privacy policies clear and distinct information that explains how the covered entity will actually use and disclose information that is in a PHR. Although there are detailed requirements for notices of privacy practices in the HIPAA Privacy Rule, they do not address the unique nature of information that is collected through or maintained in a PHR. Under the current provisions, a notice of privacy practices informs the individuals of uses and disclosures which the covered entity is legally permitted to make.[46] However, individuals need to know how an organization uses and discloses (or plans to use and disclose) information in order to make a meaningful choice between PHR services or products. Covered entities should be required to make such a privacy notice readily accessible from the entity's website page that offers PHR services.

---

[45] ARRA, § 1300(11).

[46] See 45 C.F.R. § 164.520.

Finally, it should be clarified that a covered entity that does not honor the PHR policies and practices contained in its notice of privacy practices is in violation of the Privacy Rule and is required to notify the individuals involved of the breach. By adopting these standards, HHS would bring the Privacy Rule and the breach notification rule into better alignment with the FTC breach notification rule. Such a move would go a long way toward alleviating consumer confusion that will arise out of PHRs being subject to different standards depending on the type of entity offering the service.

VII. Conclusion

We appreciate the opportunity to provide these comments in response to HHS' IFR and request for comments on the ARRA breach notification provisions that apply to HIPAA covered entities and business associates. Overall, we are concerned that the numerous exceptions to breach notification created in the IFR have the cumulative effect of undermining the intent of the statute—to inform the individual when their information is at risk using clear rules governing when notice is required, and to create incentives for covered entities to use strong policies and privacy enhancing technology such as encryption to protect data. We are also concerned that HHS' treatment of PHRs offered by covered entities does not comport with the treatment afforded in FTC's final breach notification rule and is significantly less consumer-oriented.

Accordingly, we ask HHS to:

- Revise the individual harm standard that HHS added as a trigger to the breach notification requirement, by deleting 45 C.F.R. § 164.402(1)(i) and replacing it with objective standards for judging whether the data have been "compromised" that can help entities determine whether the data are at significant risk of being inappropriately viewed, re-identified, re-disclosed, or otherwise misused.
- Issue annual or at least periodic guidance on best risk assessment practices for breach notification.
- Recognize that the potential re-identification risk of limited data sets even when dates of birth and zip codes have been removed is dependent on the receiver; determine that this information should not, as a standard matter, be given safe harbor status without any risk assessment; and eliminate or strengthen 45 C.F.R § 164.402(1)(ii) in the final version of the breach notification rule to include an assessment of risk with a high burden of proof.
- Require workforce members of covered entities who discover that they have inadvertently accessed or received information to take appropriate steps to mitigate against further use or disclosure of such information.
- Ensure PHRs will have consistent and consumer-oriented privacy and security protections for PHRs by clarifying that, with respect to a PHR offered by a covered entity or a business associate and marketed as giving consumers control over their health information, the breach definition language "unauthorized acquisition, use or disclosure," means acquisition, use or disclosure of protected health information

without the permission of the individual. Such an interpretation would bring HHS' breach notification rule in better alignment with the FTC's breach notification requirements.

- Amend the Privacy Rule so that the privacy notice of any covered entity with a PHR must clearly state the covered entity's use and disclosure of information in the PHR (as opposed to permitted uses and disclosures), and require the covered entity to abide by the terms of its notice.

These comments are jointly submitted by the Markle Foundation and the Center for Democracy & Technology and the following additional supporters:

Christine Bechtel
National Partnership for Women & Families

Hunt Blair*
Office of Vermont Health Access

Neil Calman, MD
The Institute for Family Health

Rex Cowdry, MD*
Maryland Health Care Commission

Stefanie Fenton
Intuit, Inc.

Steven Findlay

Consumers Union

Mark Frisse, MD, MBA, MSc
Vanderbilt Center for Better Health

Daniel Garrett
PricewaterhouseCoopers LLP

Gerry Hinkley, JD
Davis Wright Tremaine LLP

Joseph Kvedar, MD
Center for Connected Health, Partners Healthcare

Howard Messing
Meditech

Peter Neupert
Microsoft Corporation

Amanda Parsons, MD, MBA*
New York City Department of Health & Mental Hygiene

John Rother
AARP

Scott Schumacher, PhD
Initiate Systems, Inc.

Raymond Scott
Axolotl

Thomas Sullivan, MD
DrFirst

Robert Wah, MD
Computer Sciences Corporation

Jeb Weisman, PhD
Children's Health Fund

* Federal, state and city employees collaborate but make no endorsement.