COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to
THE FEDERAL TRADE COMMISSION
"Health Breach Notification Rulemaking"
Project No. R911002
June 1, 2009

The Federal Trade Commission (FTC) requests comment on proposed rules requiring vendors of personal health records and related entities to notify individuals when the security of their individually identifiable health information is breached.[1] The Commission must issue rules pursuant to the American Recovery and Reinvestment Act of 2009.[2]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC has a particular interest in the establishment of strong privacy safeguards for electronic health information. In October 2005, EPIC and Patient Privacy Rights launched an online campaign calling for strong privacy protections for electronic health records.[3] We found that a substantial majority of Americans consider it "very important" that their medical records be kept confidential, but fear that strong data security policies will not be implemented.[4]

We have also advised the federal courts on emerging legal issues concerning the transfer of patient record information. On August 20, 2007, EPIC filed a brief in *IMS Health v. Ayotte*, a case concerning New Hampshire's prescription privacy law.[5] EPIC's brief cited computer science research demonstrating that de-identified information is not truly anonymized, and as a result de-identification "poses significant privacy risks for patients."[6] The EPIC brief argued that there is a substantial privacy interest in de-identified patient data. Sixteen privacy and technology experts signed EPIC's brief.[7] The First Circuit eventually upheld the law, which bans the sale of prescriber-identifiable prescription drug data for marketing purposes. [8]

---

[1] Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[2] *Id*.
[3] EPIC, *EPIC and Patient Privacy Rights Launch Campaign to Protect Medical Records*, http://epic.org/press/102605.html.
[4] *Id*.
[5] *See generally* EPIC, *IMS Health Inc. v. Ayotte, Concerning the Use of Prescriber-Identifiable Data for Targeted Marketing*, http://epic.org/privacy/imshealth.
[6] Supplemental Brief for Elec. Privacy Info. Ctr. as Amicus Curiae Supporting Defendant, *IMS Health, Inc. v. Ayotte*, 550 F. 3d 42 (1st Cir. 2008) (No. 07-1945), at 10.
[7] *Id*.
[8] *Id.*

And EPIC has provided advice to Congress concerning the development of effective policies for security breach notification. In a recent hearing before the House Subcommittee on Commerce, Trade, and Consumer Protection, EPIC made several suggestions to improve breach notification, including new notification methods such as using text messaging as a supplement to letters and emails.[9] EPIC also suggested the use of Internet social networking sites to promulgate data breach notices. Such notice can supplement other "media notices," which traditionally include publication in newspapers, and conspicuous postings on websites.[10] And EPIC emphasized the importance of a centralized reporting function so that it would be possible to determine trends concerning the extent and sources of security breaches.

Scope of Rulemaking

The proposed FTC rules would require certain entities that offer personal health records (PHR) to notify consumers when the security of their health information is breached.[11] A PHR is defined as "a record that end-user consumers of healthcare can access directly online to manage their health information."[12] These regulations will apply to entities that are not subject to the Health Insurance Portability and Accountability Act (HIPAA)[13] rules promulgated by the Department of Health and Human Services (HHS). The purpose of the proposed FTC rule is to implement the American Recovery and Reinvestment Act of 2009's data breach notification requirement. The law mandates notifications by entities which are not covered under HIPAA rules, but which nonetheless possess personal health data.[14]

The main distinction that sets this proposed rule apart from the HIPAA laws is that private entities, rather than healthcare providers, are maintaining PHRs that are accessible to healthcare consumers.[15] The private entities under the proposed rule include (1) PHR vendors, (2) other PHR related entities, and (3) those vendors' and entities' third party service providers.[16] Examples of these entities would include nonprofit organizations that offer PHRs, "companies that advertise dietary supplements online, entities that offer web-based applications to help consumers manage medications, websites offering online personalized health checklists, and third party service providers such as entities that provide services such as billing or data storage

[9] *Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act,"* (May 5, 2009) (Testimony of Marc Rotenberg, EPIC House Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection) at 3.
[10] *Id*.
[11] Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[12] *The FTC's Proposed Notification Rule for Breach of Personal Health Record Information: More Consumer Protections for an Internet-Based World,* Health Law Update (Bass, Berry, & Sims PLC Attorneys at Law) May 5, 2009.
[13] 45 C.F.R. § 160.101 *et seq.* (2003).
[14] Health Breach Notification Rule, 74 Fed. Reg. 17,914 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[15] *The FTC's Proposed Notification Rule for Breach of Personal Health Record Information: More Consumer Protections for an Internet-Based World,* Health Law Update (Bass, Berry, & Sims PLC Attorneys at Law) May 5, 2009.
[16] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,917 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

to PHR-related entities or vendors of PHR."[17] Some of the most commonly known examples of these entities would include Google Health, WedMD.com, Microsoft's Health Vault, and Dossia PHR.[18]

EPIC's Comments and Recommendations

1. *The current proposed regulation is not broad enough, and should ensure that all entities handling electronic PHR are subject to the regulation.*

The proposed rule is only estimated to govern approximately 900 entities.[19] This number includes vendors of personal health records, PHR related entities, and other third party service providers.[20]

The scope of the Commission's regulatory authority should be construed as broadly as possible, and the regulation should ensure that *all* entities that handle PHRs are subject to the rules. Beyond direct vendors of personal health records, the PHR data breach provisions of the American Reinvestment and Recovery Act (ARRA) cover third party entities that "provide[] services to a vendor of personal health records."[21] This should be construed as any party that handles PHR data, including those entities that facilitate data transfer between a vendor and third party service providers. If an entity handles PHR data, it should be subject to breach-reporting requirements so that the privacy interests of citizens are protected.

Important benefits would derive from a broadened regulation. First, the Commission will be able to gain a more concrete sense of all the entities that handle PHR data. Much of this data is unknown and speculative – the proposed rule notice providing the estimate of covered entities was based on industry sources, not concrete data.[22] If rule is broadened and all such entities are required to report to the FTC, both the FTC and Congress will have more reliable data on all entities that handle PHR data.

Because the rule is explicitly subordinate to any future, general data breach notification legislation,[23] it also provides the FTC with a unique opportunity to strengthen privacy regulations

---

[17] *The FTC's Proposed Notification Rule for Breach of Personal Health Record Information: More Consumer Protections for an Internet-Based World,* Health Law Update (Bass, Berry, & Sims PLC Attorneys at Law) May 5, 2009.

[18] *See e.g.,* www.google.com/intl/en-US/health/faq.htm; http://www.webmd.com/phr; http://www.healthvault.com/; *dossia.org/consumers. (last visited Jun 6, 2009).*

[19] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,920 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

[20] *Id*.

[21] American Reinvestment and Recovery Act of 2009, Pub. L. No. 111-5, § 13,407(b), 123 Stat. 115, 269.

[22] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,920 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

[23] *See* American Reinvestment and Recovery Act of 2009, Pub. L. No. 111-5, § 13,407(g)(2),123 Stat. 115, 271. The Sunset provision of the statute authorizing the FTC's rulemaking authority states that, "[i]f Congress enacts new

covering PHR breaches, assess the strengths and weaknesses of such a regime, and file a report with Congress. The authorizing statute requires that the FTC conduct a study on privacy and security requirements for entities that are not covered under HIPAA within one year of the legislation (Feb. 17, 2010).[24] If the regulations are broad, this can become a great information-gathering opportunity for the Commission. It could, for example, examine multiple classifications of entities not covered under HIPAA and gauge the relative costs and benefits that are associated with various entities that handle PHR. If Congress receives a report that most accurately reflects the benefits consumers can receive from broad regulations (as well as potential costs), it will be in the best position to assess the necessary scope of future regulation that will adequately protect citizens' privacy interests.

A broad regulatory rule is within the scope of the statute. In Part 2 of the authorizing statute's privacy subtitle, the ARRA's text notes that the privacy standards under HIPAA "shall remain in effect to the extent that they are consistent with [the ARRA PHR privacy provisions]."[25] Thus, the ARRA's privacy protections are intended to expand existing HIPAA safeguards. Indeed, the secretary of HHS is instructed to amend any Federal regulations under HIPAA to ensure consistency with regulations promulgated under the ARRA.[26] Congress therefore contemplated experimental efforts by the agencies to enhance privacy breach notification requirements related to PHR.

Under a broad regime, we acknowledge that citizens may, at times, receive breach notifications from an unfamiliar source. In addition, there may be instances where citizens receive notifications from multiple sources. Such notifications are likely to come from third party providers and not the direct PHR vendors. Therefore, we would recommend in these cases that (a) the corresponding PHR vendor send a single breach notification to the individual in a manner that comports with our recommendations or (b) once reported by the third party entity, all third party breach notifications can come from an FTC department or office in a standardized form. Both of these solutions should require that the third party entity subsidize the costs of such notification. In all such cases, however, consumers must be informed that their privacy has been violated.

These measures would be further facilitated by a rule that requires entities to report all breaches to the FTC via some centralized means, such as an electronic reporting system or database. If reporting is consistent and centralized, redundant breach messages will be less likely because the agency will be able to filter possible redundancies in a centralized system. Thus, EPIC recommends a consistent health breach reporting framework. Under the current proposal, breaches will not be reported consistently – those breaches affecting greater than 500 persons

---

legislation establishing requirements for notification in the case of breach of security, that apply to entities that are not covered entities or business associates, the provisions of this section shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation." *Id*.

[24] § 13,424(b)(1), 123 Stat. 115 at 277

[25] § 13,421(b), 123 Stat. 115 at 276.

[26] *Id*.

must be reported within five days, while those affecting fewer than 500 persons can be logged by entities on a rolling basis and reported annually.[27]

2. *EPIC supports the presumption that if information has been accessed it has also been acquired.*

The standard of determining whether a breach has occurred is the "acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual."[28] The difference between when personal health records or information has been *accessed* or *acquired* is a matter that should be examined.

The difference between accessing and acquiring information can be ambiguous. For example, does an acquisition occur when an individual's personal health record (PHR) has been accessed by a third party (*i.e.*, accidentally coming across it in a workplace database, when the third party intended to access someone else's PHR)? Should the individual whose information was accidentally accessed be notified of such an incident? Certainly, notification is required when a PHR has been accessed and acquired, *e.g.* an outside party seeking an individual's PHR with the intention to sell this information for marketing purposes. Questions arise when information has been accessed but has not been intentionally acquired*, e.g.*. accidental disclosure of an individual's PHR resulting in increased insurance rates.

EPIC supports the proposed rule's presumption that any information that could be accessed by an unauthorized person was acquired, thus triggering notice obligations.[29] However, the proposed rule permits rebuttal of this presumption if reliable evidence demonstrates that the information could "not reasonably have been acquired."[30] This standard produces slippery slope risks, lacks a bright-line standard, and would allow PHR vendors leeway in an area where consumer protection should take precedence over the interests of PHR vendors. The default rule should state a clear, bright-line requirement for notification whenever an unauthorized person has obtained access to a PHR.

[27] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,918 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[28] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,915 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[29] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,915 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[30] *Id.*

3. The "safe harbor" for de-identified information creates significant risks to personal privacy and will undermine the purpose of the Act.

The FTC's requested additional examples of instances where there is "no reasonable basis to believe that information is individually identifiable."[31] EPIC challenges the premise on which this statement is grounded, and raises three objections. First, "de- identified" information is not necessarily anonymous – in fact, much information that has been anonymized and presumed untraceable to a person's individual identity has been later associated with a particular person. Because computer science – and the science of re-identification – continues to improve, we cannot be assured that a particular set of data will not be traced back to an individual. Second, EPIC challenges the procedural components that justify a classification of de-identified information. These procedural requirements defer too much to the entities that could experience breaches in PHRs rather than disinterested third partied that could make an objective determination as to the actual risk.. In addition, the current procedural requirements fail to provide specific guidelines on threshold requirements that would allow qualified statisticians to make determinations that a particular set of data has been adequately de-identified such that it is exempt from the rule. Finally, EPIC opposes any attempt to broaden the scope of information construed as "de-identified" and therefore exempt from the rule governing breaches.

A. Computer science has demonstrated that "de-identified" information is not truly anonymous.

Despite the fact that identifiers such as names, next of kin, Social Security Numbers, and other information are removed from data, individuals associated with such de-identified data are only anonymous to the extent that outside information cannot be obtained that allows an individuals to be linked to that record.[32] Frequently, entities can easily access databases or other information that allow them to link records across databases.

There are several instances where supposedly de-identified information has been re-identified and associated with a particular person. In Massachusetts, for example, the Group Insurance Commission (GIC) released patient specific data of state-employee health records.[33] This data did not contain the names, addresses, or Social Security numbers of any of the state employees.[34] As a result, the state agency believed this data to be anonymous.[35] However, Professor Latanya Sweeney was able to use this data and cross-reference it to publicly available voter-registration data to track down the health records of then-Governor William Weld.[36]

---

[31] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,916 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[32] *See, e.g.,* Paul Ohm, *The Probability of Privacy* [forthcoming 2009]
[33] *See* Latanya Sweeney, Testimony Before the Pennsylvania House Select Committee on Information Security, *Recommendations To Identify and Combat Privacy Problems in the Commonwealth*, October 5, 2005.
[34] *Id.*
[35] *Id.*
[36] *Id.*

In another example, AOL released search data pertaining to approximately 658,000 of its subscribers.[37] This de-identified search data was eventually traced to Thelma Arnold, a widow from Lilburn, Georgia who admitted to a reporter that she performed the searches.[38] Furthermore, researchers at The University of Texas at Austin were able to de-anonymize movie ratings data that was publicly supplied by NetFlix. Assuming that the researchers could obtain eight movie ratings from a particular person, they were able to identify that person 99% of the time.[39] With the knowledge of only two ratings and dates they could still identify the records of approximately 68% of the users in the database.[40] Most people would never assume that such information is personally identifiable, but it is. Thus, computer science has unpredictably advanced in a manner that creates additional privacy risks.

Additionally, in *IMS v. Ayotte*, EPIC filed an *amicus curiae* brief, explaining that "de-identified" patient pharmaceutical data collected by IMS Health was subject to re-identification.[41] Like the above instances, quasi-identifiers could be used for re-identification because they can be linked to external databases that contain identifying variables. Such information could be obtained through public records, as Professor Sweeney was able to do using voter registration data in the GIC example, or through birth and death certificates, as researchers were able to do in a study of Chicago's homicide database.[42]

B. The procedural requirements proposed to determine whether or not a dataset has been adequately de-identified are inadequate.

Even though the notice of this rule states that the HHS rules governing HIPAA will be applied for this particular rule,[43] the regulations do not establish a high enough threshold to protect privacy regarding "de-identified" health information. The requirements for classifying a set of data should as "de-identified," should be strengthened relative to the HIPAA standards.

First, the proposed rule states that information may be characterized as "de-identified" when there has been a formal determination by a "qualified statistician" that the information has

---

[37] Dawn Kawamoto & Elinor Mills, *AOL Apologizes for Release of User Search Data*, CNET NEWS, Aug. 7, 2006, http://news.cnet.com/AOL-apologizes-for-release-of-user-search-data/2100-1030_3-6102793.html.

[38] Michael Barbaro & Tom Zeller Jr., *A Face is Exposed For AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9 2006, http://www.nytimes.com/2006/08/09/technology/09aol.html.

[39] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*,11 (2008), www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[40] Narayanan & Shmatikov, *supra* note 27, at 11.

[41] Supplemental Brief for The Elec. Privacy Info. Ctr. as Amicus Curiae in Support of Defendant, *IMS Health Inc. v. Ayotte*, 550 F. 3d 42 (1st Cir. 2008) (No. 07-1945).

[42] *See* Salvador Ochoa et a., *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims)

[43] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,916 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318) (""[I]f a breach involves information that involves information that has been 'de-identified' under HHS rules implementing HIPAA, the Commission will deem that information to fall outside the scope of 'PHR identifiable health information' and therefore not covered by the proposed rule.").

been de-identified.[44] This clause produces privacy risks because it is not clear that such qualified statisticians will be subject to consistent guidelines to determine the bright-line between what data is or is not adequately de-identified. In addition, such statisticians may use different methodologies to make these determinations. Thus, determinations of adequate de-identification could be subject to wide variability under the rule, and entities that seek to exempt themselves from the breach reporting requirements may actively seek out "qualified statisticians" that use methodologies or techniques that minimize their notice obligations under the rule. This affords the entities covered by the rule too much of a role in determining the adequacy of de-identified data.

The proposed rule also states that the information may be characterized as "de-identified" if "specific identifiers about the individual, the individual's relatives, household members, and employers are removed, *and the covered entity has no actual knowledge that the remaining information could be used to identify the individual.*"[45] This also provides too much leeway to regulated entities. If entities use data that is not formally certified to reach a minimum threshold of de-identification, they should not be permitted to make in-house determinations that their data is de-identified. As described above, the mere removal of personal identifiers cannot be assured to protect privacy. Given the substantial interests at stake, this is not a risk to take. If entities have not undertaken measures to formally certify that data is de-identified, they should be subject to reporting requirements when that data is breached.

This rule is an opportunity to strengthen the HIPAA Privacy Rule and breach notification requirements. Under the ARRA,[46] the Department of Health and Human Services is also required to promulgate regulations that will cover entities outside of the scope of the present rulemaking. This rule, therefore, represents a unique opportunity to set out strong privacy protections for individuals whose personal health information has been compromised. While some de-identified data exemptions could be reasonable, such exemptions should be more strictly limited than those in the current proposed rule, and under no circumstance should regulated entities have authority to unilaterally determine whether data is de-identified.

C. EPIC opposes broadening the scope of de-identified information.

Given the uncertainties and privacy risks associated with de-identified data, we further object to the proposal for *additional instances* that may justify expanded classifications of de-identified data. Any broadening of notification exemptions would not outweigh the privacy interests that are implicated by such actions. Rather, as set forth above, the present exemptions should be narrowed to provide greater protections for patients. By calling for additional instances that would create de-identified data exceptions to the rule, the FTC risks narrowing the scope of consumer privacy protection while exposing the consumers to the harms that would results from re-identification and other future advances in computer science.

---

[44] *Id*.
[45] *Id.* (emphasis added).
[46] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115.

4. *Substitute media notices should be used as supplemental notification.*

Currently, when ten or more individuals cannot be reached, the regulated entity must provide data breach notifications by substitute media notice.[47] In this instance, notice can either be provided through the home page of the entity's website, or it can be provided in major print or broadcast media.[48] The proposed rule states that the posting should be "conspicuous" and posted for a period of six months.[49]

EPIC has previously advocated that new technologies such as text messaging and social networking be used to notify individuals of breaches -- wherever possible -- in addition to email and general mailings.[50] These technology platforms can reach a large mass of individuals who have not been otherwise contacted. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But it is a very effective technique for notification, and it could help make people aware that they should look for additional notice *via* physical or electronic mail.

5. *The FTC should enhance media notification.*

A. Media notification requirement should be technologically neutral, using both traditional and cutting edge media.

The proposed rule states that "if there has been a breach of security of unsecured PHR identifiable health information of 500 or more residents of the State or jurisdiction" there is a requirement of media notice "to prominent media outlets serving a State or jurisdiction."[51] We support this proposal as a supplement, but not substitution, for individual notice data breach victims.[52]

Further, EPIC encourages the FTC to look into opportunities that would improve the adequacy of notice when a breach occurs. As stated previously, expansion of media platforms and for supplemental notice would increase the effectiveness of the rule's data breach notice

[47] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,918-17,919 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318). EPIC would like to note that it is not clearly stated within the proposed rule whether this number, of ten individuals, refers to ten individuals *per breach* or aggregately. For all intents and purposes we have assumed that this number will refer to being unable to reach ten individuals *per breach*.
[48] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,919 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[49] *Id.*
[50] *Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act,"* (May 5, 2009) (Testimony of Marc Rotenberg, EPIC House Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection).
[51] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,919 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).
[52] *Id.*

requirements.[53] The rule should be flexible, allowing for the adoption of new media technologies that are able to notify populations on an even greater scale as new technological developments take place. Rather than specifying an exclusive list of media platforms for supplemental notification *e.g.* text messaging, social networking sites, newspapers, and television, the Commission should create a provision that mandates the most effective and relevant media notification method. Technology neutral rules enable the rules to keep pace with rapidly changing technologies. Cutting edge alternatives are able to contact audiences more effectively. Receiving a text message, or a Facebook alert which is personally addressed to individuals -- even if sent in a mass form -- is a more efficient approach to reach and inform individuals than the traditional newspaper or television news casting, which requires individuals to be tuning in to such news sources.

B. The FTC should establish a central location to track and announce breaches.

There is no comprehensive, central repository of information concerning PHR data breaches, or data breaches generally. As a result, reliable data is elusive, and researchers' efforts to analyze the scope and nature of data breach risks have been stymied. The FTC should establish, in this rulemaking, a central location for submission of the data breach notifications required under the present rule. Entities covered by this rulemaking should be required to forward all notifications to the Commission, and notification data should be made available to the public.

Such a resource would be of enormous utility to researchers, computer scientists, and privacy advocates. A central PHR data breach repository would also be valuable to consumers. It would enable patients to check a single resource to determine whether their personal health information has been disclosed in a data breach. A single resource for PHR data breach notifications is a useful, commonsense supplement to the targeted, though imperfect, individual notifications required by the proposed rule.

6. *The FTC should require verification that consumers receive data breach notifications.*

The FTC should require that companies verify receipt of breach notifications delivered by email. One of the Commission's explicit goals for the proposed rule is ensuring "prompt and effective notice."[54] A delivery verification requirement for email breach notifications would facilitate this goal. It would also provide a solution to the concern that these email notifications may be screened by consumers' spam filters and not delivered properly.

[53] *Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act,"* (May 5, 2009) (Testimony of Marc Rotenberg, EPIC House Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection).
[54] Health Breach Notification Rule, 74 Fed. Reg. 17,914, 17,918 (Apr. 20, 2009) (to be codified at 16 C.F.R. pt. 318).

7. *The FTC should create minimum security standards and assess penalties for violations.*

The FTC should establish comprehensive privacy and security standards, and impose penalties on PHR entities whose security protocols do not meet minimum requirements, resulting in data breaches. Also, EPIC supports the creation of a private right of action, including statutory damages and/or civil penalties, in addition to injunctive relief. In the past, EPIC has outlined the elements of comprehensive privacy and security standards. At this time, EPIC supported the implementation of "substantial criminal and civil fines" that "should be imposed for actual or attempted unauthorized access, disclosure, or use of medical information."[55] Additionally, EPIC supports individual in being able to enforce rights and obtain damages and related costs in civil court.[56] Lastly, EPIC supported the appointment of an independent agency which would be created to conduct oversight and enforce the provisions of privacy law.[57]

The availability of a cause of action will "not only provide the opportunity for individuals who have been harmed by security breaches to have their day in court, but it would also provide a necessary backstop to the current enforcement scheme which relies almost entirely on the Federal Trade Commission, acting on its own discretion and without any form of judicial review, to enforce private rights."[58] EPIC supports a private cause of action. Without a private cause of action, the enforcement burden will fall exclusively on the Commission, which has limited resources and not much success over the last few years safeguarding consumer privacy:

> If the law is passed without a private right of action, and the Commission fails to act, is reluctant to act, or simply doesn't understand a problem where it should act, individuals who are harmed by a security breach will be in a worse position than they were before the law was adopted because an any rights that were previously available under state law, [given preemption] and less those explicitly carved out, will no longer be available.[59]

In addition, this method would ensure that all PHR entities affected by the proposed rule would be more mindful in creating sufficient security for consumers, as well as providing a greater incentive for them to maintain greater protections for consumers. Imposing penalties would also minimize the risk of reoccurrence of similar incidents. These privacy-protecting incentives are established in the Do-Not-Call[60] and Junk Mail[61] laws, which provide relief to

---

[55] "Epic Alert: Principles for Federal Privacy Protections of Medical Records." Volume 2.13 http://epic.org/privacy/medical/EPIC_Principles.txt (Oct. 30, 1995).
[56] *Id.*
[57] *Id.*
[58] *Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act,"* (May 5, 2009) (Testimony of Marc Rotenberg, EPIC House Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection).
[59] *Legislative Hearing on "H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act,"* (May 5, 2009) (Testimony of Marc Rotenberg, EPIC House Commerce Committee, Subcommittee on Commerce, Trade, and Consumer Protection).
[60] 47 C.F.R. § 64.1200

consumers, provide incentives against the reoccurrence of prohibited conduct, and encourage entities to maintain consumer friendly policies that are safe and proactively protective.

EPIC acknowledges that many states have data breach laws in place, and that there are several bills pending in Congress that could affect the handling of data breaches more broadly. Nonetheless, given that PHRs are increasingly available in electronic form, EPIC supports the FTC in taking immediate steps to safeguard and proactively prevent breaches from occurring by creating minimum security standards and imposing penalties in the event of violations.

Conclusion

EPIC is pleased that Congress provided the FTC with authority to regulate entities that hold consumers personal health data, but are outside the scope of HIPAA regulations. The present rule could provide substantial new privacy protections for consumers by expanding regulatory coverage to all third parties who handle Personal Health Records, tightening exemptions for de-identified data, and mandating effective supplemental means of notification when personal health information has been compromised. As currently drafted, however, the proposed rule only covers a subset of all entities who handle PHRs, provides broad exceptions from notice requirements for data that is "de-identified" but nonetheless remains personally identifiable, and fails to take advantage of cutting edge technologies for providing supplemental breach notifications. EPIC requests that the FTC modify the proposed PHR data breach rules as set forth above.

[61] 47 U.S.C. § 227