Supporting Statement for the Health Breach Notification Rule and Form
16 C.F.R. Part 318
(OMB Control No. 3084-NEW)

On February 17, 2009, President Obama signed the American Recovery and Reinvestment Act of 2009 (the "Recovery Act" or "the Act") into law. The Act includes provisions to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information**.**

(1) & (2) Necessity for and Use of the Information Collection

Among other things, the Recovery Act recognizes that there are new types of web-based entities that collect consumers' health information. These entities include vendors of personal health records and other entities that offer online applications that interact with such personal health records ("PHR related entities"). Some of these entities are not subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act ("HIPAA"). For such entities, the Recovery Act requires the Department of Health and Human Services ("HHS") to study, in consultation with the Federal Trade Commission ("FTC" or "Commission"), potential privacy, security, and breach notification requirements and submit a report to Congress containing recommendations within one year of enactment of the Recovery Act.

The Act also requires the FTC to adopt a rule implementing the breach notification requirements applicable to vendors of personal health records, PHR related entities, and third party service providers within 180 days of enactment of the Act. It also authorizes the FTC to seek civil penalties for violations. Accordingly, the Commission has issued a final rule ("Rule") implementing these requirements. 74 Fed. Reg. 42962 (Aug. 25, 2009). The Rule requires vendors of personal health records and PHR related entities to provide: (1) notice to consumers whose unsecured personally identifiable health information has been breached; and (2) notice to the Commission. The Rule requires third party service providers (i.e., those companies that provide services such as billing or data storage) to vendors of personal health records and PHR related entities to provide notification to such vendors and PHR related entities following the discovery of a breach. The Rule does not include recordkeeping requirements. To notify the FTC of a breach, the Commission has developed a form, which it will post at www.ftc.gov/healthbreach, for entities subject to the rule to complete and return to the agency.[1] These notification requirements are subject to the provisions of the Paperwork Reduction Act, 44 U.S.C. Chapter 35 ("PRA").

Consistent with the September 24, 2009 effective date of the Rule and these notification (disclosure and reporting) requirements inclusive within it, the Commission seeks OMB

[1] An affected entity must provide notice to the Commission within ten business days of learning that the breach affected 500 people. The Commission believes that this time period still satisfies the Recovery Act's mandate that notice to the Commission be "immediate," while allowing entities additional time to investigate the circumstances surrounding the breach before notifying the FTC. See 74 Fed. Reg. at 42975.

clearance by no later than this date.[2]

(3) Information Technology

The Rule gives explicit examples of electronic options that covered entities may use to provide notice to consumers. These electronic options help minimize the burden and cost of the Rule's information collection requirements for entities subject to the Rule. They are consistent with the Government Paperwork Elimination Act ("GPEA"), which, in relevant part, requires that OMB ensure that Executive agencies, by October 23, 2003, provide for the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper. See 44 U.S.C. § 3504 note.

As mentioned above, the Commission will make available online the form entities will use to notify the Commission of a breach. The form requests minimal information, mostly in the nature of replies to check boxes. Entities can complete it online and then print and send it to a designated FTC official by courier or overnight mail. The form's simplicity and availability at the FTC's website help minimize the burden and cost of its information collection. Although it cannot be filed electronically at present,[3] the form's availability online is consistent with GPEA objectives.

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that would conflict with the Rule or its requirement that entities covered by the final rule use the form to notify the Commission of a breach. There is a potential for overlap with forthcoming rules to be promulgated by HHS governing breach notification for entities covered by HIPAA. Accordingly, the FTC consulted with HHS to harmonize the two rules, within the constraints of the statutory language. Moreover, for some entities subject to both the HHS and FTC rules, compliance with certain HHS rule requirements shall be deemed compliance with the corresponding provisions of the FTC's rule.

(5) Efforts to Minimize Small Organization Burden

In drafting the Rule, the Commission has made every effort to avoid unduly burdensome requirements for entities. In particular, the Commission believes that the alternative of providing notice to consumers electronically will assist small entities by significantly reducing the cost of sending breach notices. And, the Commission's creation of a user-friendly form

---

[2] Following section 13407(g)(1) of the Recovery Act, section 318.8 of the final rule provides that the rule shall "apply to breaches of security that are discovered on or after [insert date that is 30 days after [the publication date in the FEDERAL REGISTER 2009]." Publication occurred on August 25, 2009; hence, the effective date of September 24, 2009.

[3] Due to security concerns associated with email transmission, the Commission will not accept emailed forms at this time.

relieves entities of the separate need to design their own to notify the Commission of a breach. The form requests minimal information, mostly in the nature of replies to check boxes; thus, entities will not require extensive time to complete it. Moreover, the Commission will make the form available on its website, so that entities can fill it out online, print it out, and send it to a designated FTC official.

(6) Consequences of Conducting Collection Less Frequently

A less frequent "collection" would violate both the express statutory language and intent of the Recovery Act.

(7) Circumstances Requiring Collection Inconsistent with Guidelines

The collection of information in the Rule is consistent with all applicable guidelines contained in 5 C.F.R. § 1320.5(d)(2).

(8) Public Comments/Consultation Outside the Agency

The Commission sought through its notice of proposed rulemaking ("NPRM") public comment on the various aspects of the Rule, including the Rule's PRA implications. See 74 Fed. Reg. 17914 (April 20, 2009). The Commission discussed these comments in its preamble to the final rule. See 74 Fed. Reg. at 42976 - 42978. Moreover, the Commission has addressed in its final rule preamble the "practical utility" of the information collections of this rulemaking, in response to OMB's April 23, 2009 filed comment to that effect. See id. at 42976. In addition, FTC staff shared its draft form with HHS.

(9) Payments or Gifts to Respondents

Not applicable.

(10) & (11) Assurances of Confidentiality/Matters of a Sensitive Nature

Neither the Rule's breach notification requirements nor the associated form involve disclosure of confidential or sensitive information.

(12) Estimated Annual Hours Burden and Associated Labor Costs[4]

In the event of a data breach, the final rule requires covered firms to investigate and, if

[4] Staff notes that its estimate of the annual hours burden and labor costs likely overstates the costs imposed by the Rule because: (1) it assumes that all breaches will require notification, whereas many breaches will not require notification (e.g., those involving data that is not "unsecured"); (2) it assumes that all entities subject to the Rule's notification requirements will be required to take all of the steps described below; and (3) staff made conservative assumptions in developing many of the underlying estimates.

certain conditions are met, notify consumers and the Commission. The annual hours burden and labor costs associated with these requirements will depend on a variety of factors, including the number of covered firms that will experience a breach requiring further investigation and the number of breach notices sent.

Staff estimates that approximately 200 vendors of personal health records and 500 PHR related entities will be covered by the Commission's final Rule. Thus, an estimated 700 entities will be required to notify consumers and the Commission in the event that they discover a breach. An estimated 200 third party service providers also will be subject to the Rule, and thus required to notify vendors of personal health records or PHR related entities in the event of a breach. Thus, a total of approximately 900 entities will be subject to the final Rule's breach notification requirements.

Staff further estimates that these entities, cumulatively, will experience 11 breaches per year for which notification may be required. Because there is insufficient data at this time about the number and incidence of breaches in the PHR industry, staff used available data relating to breaches incurred by private sector businesses in order to calculate a breach incidence rate. Staff then applied this rate to the estimated total number of entities that will be subject to the final Rule. According to one recent research paper, private sector businesses across multiple industries experienced a total of approximately 50 breaches per year during the years 2002 through 2007.[5] Dividing 50 breaches by the estimated number of firms that would be subject to a breach (4,187)[6] yields an estimated breach incidence rate of 1.2% per year. Applying this incidence rate to the estimated 900 vendors of personal health records, PHR related entities, and third party service providers yields an estimate of 11 breaches per year that may require notification of consumers and the Commission.

FTC staff projects that covered firms will require on average, per breach, 100 hours of employee labor to determine what information has been breached, identify the affected customers, prepare the breach notice, and make the required report to the Commission, at an

---

[5] Sasha Romanosky, Rahul Telang & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" Seventh Workshop on the Economics of Information Security, June 2008. The authors tallied the breaches reported to the website Attrition.org during the time period 2002 to 2007 and counted a total of 773 breaches for a range of entities, including businesses, governments, health providers, and educational institutions. Staff used the volume of breaches reported for businesses (246 over a 5 year period, or approximately 50 per year) because that class of data is most compatible with other data staff used to calculate the incidence of breaches.

[6] Staff focused on firms that routinely collect information on a sizeable number of consumers, thereby rendering them attractive targets for data thieves. To do so, staff focused first on retail businesses and eliminated retailers with annual revenue under $1,000,000. The 2002 Economic Census reports that, in that year, there were 418,713 retailers with revenue of $1,000,000 or more. To apply 50 breaches to such a large population, however, would yield a very small incidence rate. In an abundance of caution, to estimate more conservatively the incidence of breach, staff then assumed that only one percent of these firms had security vulnerabilities that would render them breach targets, thus yielding the total of 4,187.

estimated cost of $4,652[7] (staff assumes that outside services of a forensic expert will also be required and those services are separately accounted for in the "Estimated Capital/Other Non-Labor Costs Burden" discussion under item (13) below). Based on the estimate that there will be 11 breaches per year, the annual employee labor cost burden for affected entities to perform these tasks was estimated to be $51,172 (11 breaches x $4,652 each).[8]

Additionally, covered entities will incur labor costs associated with processing calls that come in through the toll-free number they may set up in the event of a data breach.[9] Staff estimates that processing per breach an estimated 5,000 calls for the first month will require an average of 1,917 hours of employee labor at a cost of $27,468.[10] Affected entities will need to offer the toll-free number for an additional two months, during which time staff projects that entities will each cumulatively receive an additional 3,000 calls per breach,[11] at a cost of

---

[7] Hourly wages throughout this document are based on http://www.bls.gov/ncs/ncswage2007.htm (National Compensation Survey: Occupational Earnings in the United States 2007, U.S. Department of Labor released August 2008, Bulletin 2704, Table 3 ("Full-time civilian workers," mean and median hourly wages).

The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at $52.56 per hour; 12 hours of marketing managerial time at $53.00 per hour; 33 hours of computer programmer time at $33.77 per hour; and 5 hours of legal staff time at 54.69 per hour.

[8] Labor hours and costs pertaining to reporting to the Commission are subsumed within this total. Specifically, however, staff estimates that covered firms will require per breach, on average, 1 hour of employee labor at a cost of $54 to complete the required form. This is composed of 30 minutes of marketing managerial time at $53.00 per hour, and 30 minutes of legal staff time at 54.69 per hour, with the hourly rates based on the above-referenced BLS table. See note 7. Thus, based on 11 breaches per year for which notification may be required, the cumulative annual hours burden for covered entities to complete the notification to the Commission is 11 hours and the annual labor cost would total $594.

[9] Overall cost of a toll-free number will depend on the cost associated with T1 lines sufficient to handle the projected call volume, the cost of obtaining a toll-free telephone number and queue messaging (a service that provides rudimentary call routing), the cost of processing each call, and the telecommunication charges associated with each call. [A T1 line is a specific type of telephone line that can carry more data than traditional telephone lines.] In the NPRM, staff estimated the cost of a toll-free line for a six-month period because the proposed rule provided that entities choosing to post a message on their homepage do so for a period of six months. Because the Commission has changed this homepage posting requirement to three months (ninety days) in response to comments, staff now estimates the cost of a toll-free line for a three-month period. Labor costs for the toll-free number entail the processing costs. The non-labor costs associated with the toll-free number are covered under "Estimated Capital/Non-Labor Costs Burden" under item (13) below.

[10] The breakdown of labor hours and costs is as follows: 667 hours of telephone operator time (8 minutes per call x 5,000 calls) at $14.87 per hour and 1,250 hours of information processor time (15 minutes per call x 5,000 calls) at $14.04 per hour.

[11] Staff anticipates that the greatest influx of calls will be in the first month, and that the volume of calls will be less for the next two months. The breakdown of labor hours and costs for this two-month period is as follows: 400 hours of telephone operator time (8 minutes per call x 3,000 calls) at $14.87 per hour and 750 hours of information processor time (15 minutes per call x 3,000 calls) at $14.04 per hour. This totals

$16,478, yielding a cumulative processing labor cost of $43,946 for the three months.

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, is $95,118.

(13) **Estimated Capital/Other Non-Labor Costs Burden**[12]

Staff estimates that the capital and other non-labor costs associated with the Rule would consist of the following:[13]

1. the services of a forensic expert in investigating the breach;
2. notification of consumers via e-mail, mail, web posting, or media; and
3. other costs associated with setting up a toll-free number, if needed (i.e., costs associated with T1 lines sufficient to handle the projected call volume, the cost of obtaining a toll-free telephone number and queue messaging, and the telecommunication charges associated with each call)

Staff estimates that covered firms (breached entities) will require 30 hours of a forensic expert's time, at a cumulative cost of $2,930. This monetary sum is the product of hourly wages of a network systems and data communications analyst ($32.56), tripled to reflect profits and overhead for an outside consultant ($97.68), and multiplied by 30 hours. Based on the estimate that there will be 11 breaches per year, the annual cost associated with the services of an outside forensic expert is $32,230.

The cost of breach notifications will depend on the number of consumers contacted. Based on a recent survey, 11.6 percent of adult consumers reported receiving a breach notification during a one-year period.[14] Staff estimates that for the prospective 3-year PRA clearance, the average customer base of all vendors of personal health records and PHR related entities will be approximately two million per year. Accordingly, staff estimates that an average of 232,000 consumers per year will receive a breach notification.

Given the online relationship between consumers and vendors of personal health records

---

$16,478.

[12] As with its estimates of the annual hours burden and labor costs associated with the Rule, staff believes that its estimate of the Rule's associated capital and other non-labor costs is likely overstated for the same reasons stated in note 4 above.

[13] The instant burden estimate excludes the cost of equipment or other tangible assets of the breached firms, as those assets likely will be used, in any event, for ordinary business purposes.

[14] Ponemon Institute, "National Survey on Data Security Breach Notification," 2005. Staff believes that this estimate is likely high given the importance of data security to the personal health record industry and the likelihood that data encryption will be a strong selling point to consumers.

and PHR related entities, most notifications will be made by email and the cost of such notifications will be de minimis.[15]

In some cases, however, vendors of personal health records and PHR related entities will need to notify individuals by postal mail, either because these individuals have asked for such notification, or because the email addresses of these individuals are not current or not working. Staff estimates that the cost of notifying an individual by postal mail is approximately $2.30 per letter.[16] Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of their customers whose information is breached, the estimated cost of this notification will be $53,360 per year.

In addition, vendors of personal health records and PHR related entities sometimes may need to notify consumers by posting a message on their home page, or by providing media notice. Based on a recent study on data breach costs, staff estimates the cost of providing notice via website posting to be 6 cents per breached record, and the cost of providing notice via published media to be 3 cents per breached record.[17] Applied to the above-stated estimate of 232,000 consumers per year receiving breach notification, the estimated total annual cost of website notice will be $13,920, and the estimated total annual cost of media notice will be $6,960, yielding an estimated total annual cost for all forms of notice to consumers of $74,240.

Based on industry research, staff projects that in order to accommodate a sufficient number of incoming calls for the above-noted three-month homepage posting period, affected entities may need two T1 lines at a cost of $9,000.[18] Staff further estimates that the cost of obtaining a dedicated toll-free line and queue messaging will be $3,017.[19] In addition, according to industry research, the telecommunication charges associated with the toll-free line will be

---

[15] See National Do Not Email Registry, A Report to Congress, June 2004 n.93, available at www.ftc.gov/reports/dneregistry/report.pdf.

[16] Robin Sidel and Mitchell Pacelle, "Credit-Card Breach Tests Banking Industry's Defenses," Wall Street Journal, June 21, 2005, p.C1. Sidel and Pacelle reported that industry sources estimated the cost per letter to be about $2.00 in 2005. Allowing for inflation, staff estimates the cost to average about $2.30 per letter over the next three years of prospective PRA clearance sought from OMB.

[17] Ponemon Institute, 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, Table 2.

[18] According to industry research, the cost of a single T1 line is $1,500 per month. Two lines for three months thus would cost $9,000.

[19] Staff estimates that installation of a toll-free number and queue messaging will require 40 hours of a technician's time. Staff applied the wages of a telecommunications technician ($25.14), tripled it to reflect profits and overhead of a telecommunications firm ($75.42), and multiplied it by 40 hours to yield $3,017.

approximately $2,000.[20] Adding these costs together, staff estimates that the capital and other non-labor costs per breach for setting up a toll-free line will be $14,017. Based on the above rate of 11 breaches per year, the annual cost burden for affected entities will be $154,187 (11 x $14,017).

In sum, the total estimate for capital and other non-labor costs is $260,657: $32,230 (services of a forensic expert) + $74,240 (costs of notifying consumers) + $154,187 (capital and other non-labor costs associated with a toll-free line).

(14) Estimate of Cost to Federal Government

Staff estimates that the cost to the FTC Bureau of Consumer Protection of enforcing the Rule's notification requirements will be approximately $270,000 per year. This estimate is based on the assumption that 3 full attorney work years will be expended to enforce the Rule's requirements related to notification. Clerical and other support services are also included in this estimate.

(15) Program Changes or Adjustments

Not applicable. This is a new information collection.

(16) Plans for Tabulation and Publication

There are no plans to publish for statistical use any information required by the Rule, but the Commission intends to input the information it receives from entities that have completed the associated form into a database, which it will update periodically and make publicly available.

(17) Display of Expiration Date for OMB Approval

Not applicable.

(18) Exceptions to Certification

Not applicable.

[20] Staff estimates a cost per call of 25¢ (5¢ per minute/per call x 5 minutes per call). Assuming 8,000 calls for each breach, the total estimated telecommunications charges are $2,000.