Supporting Statement for the
Health Breach Notification Rule and Form
16 C.F.R. § 318
(OMB Control No. 3084-0150)

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

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 included provisions to advance the use of health information technology and, at the same time, strengthen privacy and security protections for health information. The Act required the FTC to adopt a rule implementing the breach notification requirements applicable to vendors of personal health records, "PHR related entities,"[1] and third party service providers. The Commission issued a final rule on August 25, 2009. 74 Fed. Reg. 42,962.

The Health Breach Notification Rule (Rule), 16 CFR § 318, 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 only applies to electronic health records and does not include recordkeeping requirements. 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. To notify the FTC of a breach, the Commission developed a form, which is posted at www.ftc.gov/healthbreach, for entities subject to the rule to complete and return to the agency.

These notification requirements are subject to the provisions of the Paperwork Reduction Act ("PRA"), 44 U.S.C. Chapter 35. In the Commission's view, it has maximized the practical utility of the breach notification requirements in the Rule, consistent with the requirements of the Recovery Act. Section 318.4(a) of the Rule requires that consumers whose information has been affected by a breach of security receive notice of it "without unreasonable delay and in no case later than 60 calendar days" after discovery of the breach. Among other information, the notices must provide consumers with steps they can take to protect themselves from harm. Moreover, the breach notice requirements encourage entities to safeguard the information of their customers, thereby potentially reducing the incidence of harm.

The form entities must use to inform the Commission of a security breach requests minimal information, mostly as replies to check boxes; thus, entities do not require extensive time to complete it. For breaches involving the health information of 500 or more individuals, entities

[1] "PHR related entity" means an entity, other than an entity covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA-covered entity') or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) Offers products or services through the Web site of a vendor of personal health records; (2) offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or (3) accesses information in a personal health record or sends information to a personal health record. 16 CFR § 318.2(f).

must notify the Commission as soon as possible, and in any event no later than ten business days after discovering the breach. Breaches involving the information of fewer than 500 individuals may be reported in an annual submission that includes all breaches within the calendar year that fall within this category. The form serves the Commission by providing the agency with information about breaches occurring in the PHR industry. The Commission inputs the information it receives from entities into a database that the Commission updates periodically. The Commission makes certain information about these breaches available to the public. This publicly available information serves businesses and the public. It provides businesses with information about potential causes of data breaches, which is particularly helpful to those setting up data security procedures. It also provides the public with information about the extent of data breaches. Thus, in the Commission's view, the Rule and form have significant practical utility.

(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"), 44 U.S.C. § 3504 note, which, in relevant part, requires that OMB ensure that Executive agencies provide for the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper.

As noted above, the Commission makes available online the form entities will use to notify the Commission of a breach. Pursuant to § 318.5 of the Rule, entities must notify the FTC "according to instructions at the Federal Trade Commission's Web site." As of October 2015, the Commission offers a secure online method for receiving these notices. Alternatively entities may continue to print and send the form 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.

(4) Efforts to Identify Duplication

The FTC has not identified any other federal statutes, rules, or policies currently in effect that conflicts with the Rule or its requirement that affected entities use the form to notify the Commission of a breach. Due to the potential for overlap with the Department of Health and Human Service's ("HHS") Breach Notification Rule, 45 CFR §§ 164.400-414, which governs breach notification for entities covered by HIPAA, the FTC consulted with HHS to harmonize the two rules, within the constraints of the statutory language.

(5) Efforts to Minimize Small Organization Burden

In drafting the Rule, the Commission 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 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. Moreover, the Commission makes the form available on its website, so that entities can fill it out online, and either submit electronically or print 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

As required by the PRA, the FTC provided opportunity for public comment before requesting that OMB extend the existing paperwork clearance for the Rule. 44 U.S.C. 3506(c)(2)(A). See 80 Fed. Reg. 62,530 (October 16, 2015). The Commission received three comments. None of these however addressed either the burden associated with the Rule or any of the other issues raised by the public comment request.

(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

In the event of a data breach, the Rule requires covered firms to investigate and, if 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; the percentage of such firms that will experience a breach requiring further

investigation and, if necessary, the sending of breach notices; and the number of consumers notified.[2]

At the time the Rule was issued, insufficient data was available about the incidence of breaches in the PHR industry. Accordingly, staff based its burden estimate on data pertaining to private sector breaches across multiple industries. Staff estimated that there would be 11 breaches per year requiring notification of 232,000 consumers.[3]

As described above, the Rule requires covered entities that have suffered a breach to notify the Commission. Since the Rule has now been in effect for over five years, staff is now able to base the burden estimate on the actual notifications received from covered entities, which include the number of consumers notified. Accordingly, staff has used this information to update its burden estimate.

On average, about 2,500 consumers per year received notifications over the years 2010 and 2011. In 2012 and 2013, between 4,000 and 5,000 consumers received notifications each year. In 2014, approximately 17,993 consumers received notifications. In light of this upwards trend, staff bases its current burden estimate on an assumed two breach incidents per year that, together, require the notification of approximately 40,000 consumers. This estimate will likely overstate the burden; however, as consumers increasingly download their information into personal health records,[4] staff anticipates that the number of affected consumers will increase.

Estimated Annual Hours Burden: 3,267.

As explained in more detail within the next section, 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. Based on an estimated 2 breaches per year, yearly hourly burden would be 200 hours. Additionally, staff expects covered firms will require 3,067 annual hours (1,067 hours of telephone operator time + 2000 hours of information processor time) to process calls they may receive in the event of a data breach. *See* footnote 7 *infra*.

Estimated Annual Labor Costs: $61,764.

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

---

[2] The annual hours and cost estimates below likely overstate the burden because, among other things, they assume, though it is not necessarily so, that all breaches subject to the Rule's notification requirements will be
required to take all of the steps described below.

[3] 74 FR at 42977.

[4] *See e.g.*, http://www.va.gov/bluebutton/.

customers, prepare the breach notice, and make the required report to the Commission, at an estimated cost of $5,732[5](staff assumes that outside services of a forensic expert will also be required and those services are separately accounted for under "Estimated Annual Non-Labor Costs" below). Based on an estimated 2 breaches per year, the annual employee labor cost burden for affected entities to perform these tasks is $11,464.[6]

Additionally, covered entities will incur labor costs associated with processing calls they may receive in the event of a data breach. The rule requires that covered entities that fail to contact 10 or more consumers because of insufficient or out-of-date contact information must provide substitute notice through either a clear and conspicuous posting on their Web site or media notice. Such substitute notice must include a toll-free number for the purpose of allowing a consumer to learn whether or not his/her information was affected by the breach.

Individuals contacted directly will have already received this information. Staff estimates that no more than 10 percent of affected consumers will utilize the offered toll-free number. Thus, of the 40,000 consumers affected by a breach annually, staff estimates that 4,000 may call the companies over the 90 days they are required to provide such access. Staff additionally projects that 4,000 additional consumers who are not affected by the breach will also call the companies during this period. Staff estimates that processing all 8,000 calls will require an average of 3,067 hours of employee labor at a cost of $50,300.[7]

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, are $61,764.

---

[5] Hourly wages throughout this document are based on mean hourly wages found at http://www.bls.gov/news.release/ocwage.htm ("Occupational Employment and Wages–May 2014," U.S. Department of Labor, released March 2015, Table 1 ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2014").

The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at approximately $66 per hour; 12 hours of marketing manager time at $66 per hour; 33 hours of computer programmer time at $40 per hour; and 5 hours of legal staff time at $64 per hour.

[6] Labor hours and costs pertaining to reporting to the Commission are subsumed within this total. Specifically, staff estimates that covered firms will require per breach, on average, 1 hour of employee labor at an approximate cost of $65 to complete the required form. This is composed of 30 minutes of marketing managerial time at $66 per hour, and 30 minutes of legal staff time at $64 per hour, with the hourly rates based on the above-referenced Department of Labor table. *See* note 5, *supra.* Thus, based on 2 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 2 hours and the annual labor cost is approximately $130.00.

[7] This assumes telephone operator time of 8 minutes per call and information processor time of 15 minutes per call. The cost estimate above is arrived at as follows: 1,067 hours of telephone operator time (8 minutes per call × 8,000 calls) at $19 per hour, and 2,000 hours of information processor time (15 minutes per call × 8,000 calls) at $15 per hour.

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

Commission staff anticipates that capital and other non-labor costs associated with the Rule will consist of the following:

1. The services of a forensic expert in investigating the breach;
2. notification of consumers via email, mail, web posting, or media; and
3. the cost of setting up a toll-free number, if needed.

Staff estimates that covered firms (breached entities) will require 30 hours of a forensic expert's time, at a cumulative cost of $3,960 for each breach. This is the product of hourly wages of an information security analyst ($44), tripled to reflect profits and overhead for an outside consultant ($132), and multiplied by 30 hours. Based on the estimate that there will be 2 breaches per year, the annual cost associated with the services of an outside forensic expert is $7,920.

As explained above, staff estimates that an average of 40,000 consumers per year will receive a breach notification. Given the online relationship between consumers and vendors of personal health records and PHR related entities, most notifications will be made by email and the cost of such notifications will be minimal.[8]

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 a mailed notice is $0.06 for the paper and envelope, and $0.49 for a first class stamp. Assuming that vendors of personal health records and PHR related entities will need to notify by postal mail 10 percent of the 40,000 customers whose information is breached, the estimated cost of this notification will be $2,200 per year.[9]

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 Web site posting to be $0.06 per breached record, and the cost of providing notice via published media to be $0.03 per breached record.[10] Applied to the above-stated estimate of 40,000 affected consumers, the estimated total annual cost of Web site notice will be $2,400, and the estimated total annual cost of media notice will be $1,200, yielding an estimated total annual cost for all forms of notice to consumers of $5,800.

---

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

[9] As mentioned above, covered entities will also need to notify the Commission either through an online process or via mail. Staff estimates the non-labor costs for this notification to be negligible.

[10] Ponemon Institute, 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions, Table 2. In studies conducted for subsequent years, the Ponemon Institute does not report this level of detail.

Finally, staff estimates that the cost of providing a toll-free number will depend on the costs associated with T1 lines sufficient to handle the projected call volume and the cost of obtaining a toll-free telephone number.[11] Based on industry research, staff projects that affected entities may need two T1 lines at a cost of $9,000 for the 90 day period.[12] In addition, staff estimates the cost of obtaining a dedicated toll-free line to be $4,540 per month. Accordingly, staff projects that the cost of obtaining two toll-free lines for 90 days will be $27,240,[13] and the total annual cost for providing a toll-free number will be $36,240.

In sum, the total estimate for non-labor costs is $49,960: $7,920 (services of a forensic expert) + $5,800 (costs of notifying consumers) + $36,240 (cost of providing a toll-free number).

(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 $75,000 per year. This estimate is based on the assumption that 50% of one attorney work year will be expended to enforce the Rule's requirements related to notification. Employee benefits, as well as clerical and other support services, are also included in this estimate.

(15) Program Changes or Adjustments

The annual time and cost burden have been adjusted upward because the FTC anticipates more consumers will receive breach notifications. Since the Rule has now been in effect for over five years, staff has more information relating to the actual notifications received from covered entities. This includes the number of consumers that the covered entities notified. In 2012, the FTC estimated that an average of 2,500 consumers per year received notifications over the years 2010 and 2011. In 2015-2016, the FTC estimates approximately 20,000 consumers will receive notices per year.

[11] Staff included costs associated with obtaining a T1 line (a specific type of telephone line that can carry more data than traditional telephone lines) in its initial estimate in 2009, but did not include these costs in its most recent estimate based on the low number of consumers notified pursuant to the Rule in 2010 and 2011. Since staff's current estimate includes larger projected call volumes, however, staff has again included these costs. Staff recognizes that this likely overstates the burden because entities may already have these services in place and/or they may not all be necessary depending on how many consumers are affected.

[12] According to industry research, the cost of a single T1 line is $1,500 per month.

[13] Staff estimates a monthly charge of $15 along with an activation charge of $15 for each toll-free line, as well as a per minute charge of $.07. Since staff estimates each breach will require 1067 hours of telephone operator time (*see* note 7, *infra*), staff estimates the cost/month of each toll-free line to be $4,540.

(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.