This document is scheduled to be published in the
Federal Register on 10/16/2015 and available online at
http://federalregister.gov/a/2015-26362, and on **FDsys.gov**

BILLING CODE: 6750-01-S

FEDERAL TRADE COMMISSION

Agency Information Collection Activities;

Proposed Collection; Comment Request

AGENCY: Federal Trade Commission (FTC or Commission).

ACTION: Notice.

SUMMARY: The information collection requirements described below will be submitted to the Office of Management and Budget (OMB) for review, as required by the Paperwork Reduction Act (PRA). The FTC seeks public comments on its proposal to extend, for three years, the current PRA clearance for information collection requirements contained in the rules and regulations under the Health Breach Notification Rule. This clearance expires on March 31, 2016.

DATES: Comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Interested parties may file a comment online or on paper by following the instructions in the Request for Comments part of the SUPPLEMENTARY INFORMATION section below. Write "Health Breach Notification Rule, PRA Comments, P-125402" on your comment, and file your comment online at https://ftcpublic.commentworks.com/ftc/healthbreachnotificationpra by following the instructions on the web-based form. If you prefer to file your comment on paper, mail or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW, Suite CC-5610 (Annex J), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610 (Annex J), Washington, DC 20024.

FOR FURTHER INFORMATION CONTACT: Requests for copies of the collection of information and supporting documentation should be addressed to Cora Tung Han, 202-326-2441, Attorney, Privacy & Identity Protection, Bureau of Consumer Protection, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

SUPPLEMENTARY INFORMATION:

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, and the Commission issued a final rule on August 25, 2009. 74 FR 42962.

The Health Breach Notification Rule (Rule), 16 CFR Part 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 PRA, 44 U.S.C. Chapter 35. Under the PRA, federal agencies must get OMB approval for each collection of information they conduct, sponsor, or require. "Collection of information" means agency

[1] "PHR related entity" means an entity, other than a 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 website of a vendor of personal health records; (2) offers products or services through the websites 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).

requests or requirements to submit reports, keep records, or provide information to a third party. 44 U.S.C. 3502(3); 5 CFR 1320.3(c). As required by Section 3506(c)(2)(A) of the PRA, the FTC is providing this opportunity for public comment before requesting that OMB extend the existing PRA clearance for the information collection requirements associated with the Commission's rules and regulations under the Health Breach Notification Rule (or Rule), 16 CFR Part 318 (OMB Control Number 3084-0150).

The FTC invites comments on: (1) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (2) the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on those who are to respond. All comments must be received on or before [insert date 60 days after date of publication in the FEDERAL REGISTER].

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. Under the Rule, 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 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.

Pursuant to § 318.5 of the Rule, entities must notify the FTC "according to instructions at the Federal Trade Commission's Web site." In 2009, the Commission indicated that "[d]ue to security concerns associated with email transmission, the Commission will not accept emailed

forms at this time."[2] The Commission now offers a secure online method for receiving these notices, and instructions are on the form entities should use for notification, which is available on the FTC's website. Alternatively entities may continue to print and send the form to a designated FTC official by courier or overnight mail.

Burden Estimates

The PRA burden of the Rule's requirements depends 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. 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.

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

---

[2] 74 FR at 42975.

[3] 74 FR at 42977.

notify the Commission. Since the Rule has now been in effect for over five years,[4] 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,[5] 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

[4] The rule became effective on September 24, 2009. Full compliance was required by February 22, 2010.

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

process calls they may receive in the event of a data breach. *See* footnote 8 *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 customers, prepare the breach notice, and make the required report to the Commission, at an estimated cost of $5,732[6] (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.[7]

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

---

[6] 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.

[7] 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 6, *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.

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.[8]

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, is $62,000.

Estimated Annual Capital and other Non-Labor Costs: $49,960

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 e-mail, mail, web posting, or media; and
3. the cost of setting up a toll-free number, if needed.

---

[8] 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 x 8,000 calls) at $19 per hour, and 2000 hours of information processor time (15 minutes per call x 8,000 calls) at $15 per hour.

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.[9]

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.[10]

---

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

[10] 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.

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 $0.06 per breached record, and the cost of providing notice via published media to be $0.03 per breached record.[11] Applied to the above-stated estimate of 40,000 affected consumers, the estimated total annual cost of website 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.

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.[12] 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.[13] In addition, staff estimates the cost of obtaining a dedicated toll-free line to be $4,540 per month. Accordingly,

---

[11] 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.

[12] 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.

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

staff projects that the cost of obtaining two toll-free lines for 90 days will be $27,240,[14] 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).

The total estimated PRA annual cost burden is $61,764 (labor costs) + $49,960 (non-labor costs) = approximately $112,000 (rounded to the nearest thousand).

Request for Comments

You can file a comment online or on paper. Write "Health Breach Notification Rule, PRA Comments, P-125402" on your comment. Your comment -- including your name and your state -- will be placed on the public record of this proceeding, including, to the extent practicable, on the public Commission website, at http://www.ftc.gov/os/publiccomments.shtm. As a matter of discretion, the Commission tries to remove individuals' home contact information from comments before placing them on the Commission website.

Because your comment will be made public, you are solely responsible for making sure that your comment does not include any sensitive personal information, such as a Social Security number, date of birth, driver's license number or other state identification number or foreign country equivalent, passport number, financial account number, or credit or debit card number.

---

[14] 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 10, *infra*), staff estimates the cost/month of each toll-free line to be $4,540.

You are also solely responsible for making sure that your comment does not include any sensitive health information, such as medical records or other individually identifiable health information. In addition, do not include any "[t]rade secret or any commercial or financial information which is . . . privileged or confidential," as discussed in Section 6(f) of the FTC Act, 15 U.S.C. 46(f), and FTC Rule 4.10(a)(2), 16 CFR 4.10(a)(2). In particular, do not include competitively sensitive information such as costs, sales statistics, inventories, formulas, patterns, devices, manufacturing processes, or customer names.

If you want the Commission to give your comment confidential treatment, you must file it in paper form, with a request for confidential treatment, and you must follow the procedure explained in FTC Rule 4.9(c), 16 CFR 4.9(c). Your comment will be kept confidential only if the FTC General Counsel, in his or her sole discretion, grants your request in accordance with the law and the public interest. Postal mail addressed to the Commission is subject to delay due to heightened security screening. As a result, the Commission encourages you to submit your comments online. To make sure that the Commission considers your online comment, you must file it at https://ftcpublic.commentworks.com/ftc/healthbreachnotificationpra by following the instructions on the web-based form. If this Notice appears at http://www.regulations.gov, you also may file a comment through that website.

If you file your comment on paper, write "Health Breach Notification Rule, PRA Comments, P-125402" on your comment and on the envelope, and mail it to the following address: Federal Trade Commission, Office of the Secretary, 600 Pennsylvania Avenue, NW,

Suite CC-5610, (Annex J), Washington, DC 20580, or deliver your comment to the following address: Federal Trade Commission, Office of the Secretary, Constitution Center, 400 7th Street, SW, 5th Floor, Suite 5610, (Annex J), Washington, DC 20024. If possible, submit your paper comment to the Commission by courier or overnight service.

The FTC Act and other laws that the Commission administers permit the collection of public comments to consider and use in this proceeding as appropriate. The Commission will consider all timely and responsive public comments that it receives on or before [insert date 60 days after date of publication in the FEDERAL REGISTER]. You can find more information, including routine uses permitted by the Privacy Act, in the Commission's privacy policy, at http://www.ftc.gov/ftc/privacy.htm.

David C. Shonka,
Principal Deputy General Counsel

[FR Doc. 2015-26362 Filed: 10/15/2015 08:45 am; Publication Date: 10/16/2015]