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 (OMB Control Number 3084-0150), 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. Under the Rule, consumers whose information has been affected by a breach receive notice "without unreasonable delay and in no case later than 60 calendar days"[2] after discovery of the breach. Among other information, the notices must provide consumers with steps they can take to protect themselves from harm. To notify the FTC of a breach, the Commission developed a simple, two-page form requesting minimal information and consisting mainly of check boxes, which is posted at www.ftc.gov/healthbreach. 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. Entities may report all breaches involving the information of fewer than 500 individuals in an annual submission for the calendar year. The Commission uses entities' notifications to compile a list of breaches affecting 500 or more individuals that is publicly available on the FTC's website. The list provides businesses with information about potential sources of data breaches, which is helpful to those developing data security procedures. It also provides the public with information about the extent of data breaches.

The Rule also 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 only applies to electronic health records and does not include recordkeeping requirements.

---

[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).

[2] 16 CFR § 318.4(a).

(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 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 online forms available that the entities may use to notify the Commission of a breach. The Commission offers a secure online method for receiving these notices. Alternatively, entities may 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. In addition, the Commission's provision 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 and allows submissions by either electronic file transfer or mail, at the entity's preference.

(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 84 Fed. Reg. 2,868 (February 8, 2019). The Commission received seven non-germane comments that did not address 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

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 covered firms experiencing breaches subject to the Rule's notification requirements will be required to take all of the steps described below.

The analysis may also overstate the burden of the Rule's requirements because it assumes that covered firms would not take any of the steps described were it not for the requirements of the Rule. For example, the analysis incorporates labor costs associated with understanding what information has been breached. It seems likely that some firms would incur such costs even in the absence of the Rule's requirements because the firms are independently interested in identifying, understanding, and remediating security risks. A company that investigates, for its own purposes, what information has been breached is unlikely to fully duplicate the costs of that investigation in complying with the Rule. Therefore, it may not be correct in all cases that complying with the Rule results in added labor costs for this activity. Nevertheless, in order to allow for a complete understanding of all the potential costs associated with compliance, these costs are included in this analysis.

At the time the Rule was issued in 2009, 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.

In 2016, based on available data from the years 2010 through 2014, staff arrived at new estimates, projecting an average of two breaches per year affecting a total of 40,000 individual consumers.

The Rule has now been in effect for over eight years, and new data regarding the number and scale of reported breaches from 2015 through 2017 allow staff to update its burden estimates. A review of the breach reports received by the FTC from 2010 through 2017 reveals that there are two primary categories of breaches reported: (1) "single-person breaches," incidents in which a single individual's information is potentially compromised; and (2) what are hereafter described as "major breaches," in which multiple—and typically, many—individuals are affected. These two categories of breaches are addressed separately in this analysis because the frequency and costs of the categories differ significantly.

Nearly all of the submissions received between 2010 and 2017—over 99.99% of them—reported single-person breaches related to an individual's loss of control over his or her login credentials. The rate of such breaches has increased significantly since the Rule went into effect; the year-to-year average rate of increase during this period was nearly 70%. Whereas from 2011 to 2014 the average annual number of single-person breaches was 7,502, from 2014 to 2017 the average was almost 15,000. Assuming that this rate of increase continues, staff estimates that between 2019 and 2022 the agency will receive, on average, about 25,000 single-person breach reports per year.

By contrast, major breach reports are quite infrequent. On average, the FTC receives one major breach report approximately every two and a half years, with an average of approximately 200,000 persons affected. Given the low frequency at which major breaches occur, FTC staff are unable to identify any meaningful trends in the frequency of major breach reports. FTC staff has not identified any existing research allowing us to make specific projections about future variation in the frequency of major breaches. Consequently, FTC staff has assumed that the average frequency and scale of major breaches will remain more or less static. Staff's calculations are based on the estimate that a major breach will occur approximately every two and a half years and that 200,000 people will be affected by each major breach, for an annual average of 80,000 individuals affected per year.

Estimated Annual Burden Hours: 4,779.

As explained in more detail within the next section, FTC staff projects that the employee time required for each single-person breach is quite minimal because the processes for notifying consumers are largely automated and single-person breaches can be reported to the FTC in an aggregate annual notification using the FTC's two-page form. On average, staff estimates that covered firms will require approximately 20 seconds of employee labor per single-person breach. With an estimated 25,000 single-person breaches per year, the total estimated burden hours for single-person breaches is approximately 139 hours.

For each major breach, covered firms will require on average 100 hours of employee labor to determine what information has been breached, the identification of affected customers, preparation of the breach notice, and submission of the required report to the Commission.

Based on staff's estimate that one major breach occurs every two and a half years, the average annual burden of major breaches amounts to 40 hours per year.

Additionally, covered firms will incur labor costs associated with processing calls they may receive in the event of a major breach. The Rule requires that covered firms 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 200,000 consumers affected by a major breach, staff estimates that 20,000 may call the companies over the 90 days they are required to provide such access. Staff additionally projects that 10,000 additional consumers who are not affected by the breach will also call the companies during this period. Staff estimates that processing all 30,000 calls will require an average of 11,500 hours of employee labor resulting in an average annual burden of 4,600 labor hours.

Given the low frequency of major breaches, the annual average requirement for major breaches is 4,640 hours.

The combined annual hours burden for both single-person and major breaches therefore is 4,779 (4,640 + 139).

Estimated Annual Labor Costs: $96,656.

For each single-person breach, FTC staff estimates that the average 20 seconds of employee labor to provide (likely automated) notification to affected individuals and produce an annual breach notification for submission to the FTC will cost approximately $0.27 per breach. With an estimated 25,000 single-person breaches per year, the annual labor costs associated with all single-person breaches come to $6,750.

For major breaches, FTC staff projects that the average 100 hours of employee labor costs (excluding outside forensic services, discussed below as estimated non-labor costs) to determine what information has been breached, identify the affected customers, prepare the breach notice, and report to the Commission will cost an average of $62.66 per hour for a total of $6,266.[3] Based on an estimated one breach every two and a half years, the annual employee labor cost burden for affected entities to perform these tasks is $2,506.

[3] 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 2018," U.S. Department of Labor, released March 2019, Table 1 ("National employment and wage data from the Occupational Employment Statistics survey by occupation, May 2018"). The breakdown of labor hours and costs is as follows: 50 hours of computer and information systems managerial time at approximately $73 per hour; 12 hours of marketing manager time at $71 per hour; 33 hours of computer programmer time at $43 per hour; and 5 hours of legal staff time at $69 per hour.

Additionally, staff expects covered firms will require, for each major breach, 11,500 hours of labor associated with answering consumer telephone calls at a cost of $218,500.[4] Since a major breach occurs approximately every two and a half years, the average annual burden of 4,600 labor hours results in annualized labor cost of approximately $87,400.

Accordingly, estimated cumulative annual labor costs, excluding outside forensic services, for both single-person and major breaches, is $96,656 ($87,400 + $2,506 + $6,750).

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

Commission staff estimates that capital and other non-labor costs associated with single-person breaches will be negligible. Companies generally use automated notification systems to notify consumers of single-person breaches. Automated notifications are typically delivered by email or other electronic methods. The costs of providing such electronic notifications are minimal.

Commission staff anticipates that capital and other non-labor costs associated with major breaches 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.

Staff estimates that, for each major breach, covered firms will require 240 hours of a forensic expert's time, at a cumulative cost of $35,280 for each breach. This estimate is based on a projection that an average major breach will affect approximately 20 machines and that a forensic analyst will require about 12 hours per machine to conduct his or her analysis. The projected cost of retaining the forensic analyst consists of the hourly wages of an information security analyst ($49), tripled to reflect profits and overhead for an outside consultant ($147), and multiplied by 240 hours. Based on the estimate that there will be one major breach every two and a half years, the annual cost associated with the services of an outside forensic expert is $14,112.

As explained above, staff estimates that an average of 200,000 consumers will be entitled to notification of each major breach. 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.

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 $0.11 for the paper and envelope, and $0.55 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 200,000 customers whose information is

[4] The cost of telephone operators is estimated at $19/hour.

breached, the estimated cost of this notification will be $13,200 per breach. The annual cost will be around $5,280.

In addition, vendors of personal health records and PHR related entities may need to notify consumers by posting a message on their home page, or by providing media notice. Staff estimates the cost of providing notice via website posting to be $0.08 per breached record, and the cost of providing notice via published media to be $0.04 per breached record. Applied to the above-stated estimate of 200,000 affected consumers, the estimated total cost of website notice will be $16,000, and the estimated total cost of media notice will be $8,000, yielding an estimated total per-breach cost for both forms of notice to consumers of $24,000. Annualized, this number is approximately $9,600 per year.

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. Based on industry research, staff projects that affected entities may need two T1 lines at a cost of $1,800 for the 90-day period. In addition, staff estimates the cost of obtaining a dedicated toll-free line to be $100 per month. Accordingly, staff projects that the cost of obtaining two toll-free lines for 90 days will be $2,400. The total annualized cost for providing a toll-free number will be $960.

In sum, the total annual estimate for non-labor costs associated with major breaches is $29,952: $14,112 (services of a forensic expert) + $5,280 (cost of mail notifications) + $9,600 (cost of website and media notice) + $960 (cost of providing a toll-free number). Negligible non-labor costs are associated with single-person breaches.

(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 as follows—

	2016	**2019**
Annual Hours	3,267	4,779
Annual Labor and non-Labor Costs	$111,724	$126,608

from 3,267 annual hours in 2016 to 4,779 annual hours in 2019 and from $111,724 in annual labor and non-labor costs in 2016 to $126,608 annual labor and non-labor costs in 2019.

(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 about breaches affecting 500 or more individuals 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