V. Regulatory Impact Analysis

A. Executive Order 12866 and Related Executive Orders on Regulatory Review

The Department of Health and Human Services (HHS or "Department") has examined the effects of this proposed rule under Executive Order (E.O.) 12866, Regulatory Planning and Review,[1] E.O. 13563, Improving Regulation and Regulatory Review,[2] E.O. 14094, Modernizing Regulatory Review,[3] the Regulatory Flexibility Act[4] (RFA), the Unfunded Mandates Reform Act of 1995[5] (UMRA), and E.O. 13132 on Federalism.[936] E.O.s 12866 and 13563 direct the Department to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; distributive effects; and equity). The proposed rule meets the criteria as significant under section 3(f)(1) of E.O. 12866, as amended by E.O. 14094.

The RFA requires us to analyze regulatory options that would minimize any significant effect of a rule on small entities. As discussed in greater detail below, this analysis concludes, and the Secretary certifies, that the notice of proposed rulemaking (NPRM), if adopted, would not result in a significant economic effect on a substantial number of small entities.

The UMRA (section 202(a)) generally requires us to prepare a written statement, which includes an assessment of anticipated costs and benefits, before proposing "any rule that includes any Federal mandate that may result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any 1 year."[6] The current threshold after adjustment for inflation is $183 million, using the most current (2024) Implicit Price Deflator for the Gross Domestic Product. UMRA

---

[1] 58 FR 51735 (Oct. 4, 1993).
[2] 76 FR 3821 (Jan. 21, 2011).
[3] 88 FR 21879 (Apr. 11, 2023).
[4] Pub. L. 96–354, 94 Stat. 1164 (Sept. 19, 1980) (codified at 5 U.S.C. 601–612).
[5] Pub. L. 104–4, 109 Stat. 48 (Mar. 22, 1995) (codified at 2 U.S.C. 1501). [936]
64 FR 43255 (Aug. 4, 1999).
[6] Sec. 202 of Pub. L. 104–4, 109 Stat. 64 (Mar. 22, 1995) (codified at 2 U.S.C. 1532(a)).

does not address the total cost of a rule. Rather, it addresses certain categories of cost, mainly Federal mandate costs resulting from imposing enforceable duties on State, local, or Tribal governments or the private sector; or increasing the stringency of conditions in, or decreasing the funding of, State, local, or Tribal governments under entitlement programs.

This proposed rule, if adopted, would impose mandates that would result in the expenditure by State, local, and Tribal governments, in the aggregate, or by the private sector, of more than $183 million in any one year. The impact analysis in this proposed rule addresses such effects both qualitatively and quantitatively. Each covered entity and business associate (collectively, "regulated entity"), including government entities that meet the definition of covered entity (*e.g.*, State Medicaid agencies), would be required to: conduct a Security Rule compliance audit; report to covered entities or business associates, as applicable, upon activation of their contingency plan; deploy multi-factor authentication (MFA) in and penetration testing of relevant electronic information systems; complete network segmentation; disable unused ports and remove extraneous software; update cybersecurity policies and procedures; revise business associate agreements; and update workforce training. Business associates would be required to conduct an analysis and provide verification of their compliance with technical safeguards and covered entities would be required to obtain verification from business associates (and business associates from their subcontractors). Additionally, group health plans would need to revise plan documents to require plan sponsors to comply with administrative, physical, and technical safeguards according to the Security Rule standards. Finally, through contractual language, health plan sponsors would need to enhance safeguards for electronic protected health information (ePHI) according to the Security Rule standards. Costs for all regulated entities to change their policies and procedures alone would increase costs above the UMRA threshold in one year, and costs of health plan sponsors would increase total costs further. Although Medicaid makes Federal matching funds available for States for certain administrative costs, these are limited to costs specific to operating the Medicaid program. There are no Federal funds directed at Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance activities.

The Department believes that pursuant to Subtitle E of the Small Business Regulatory Enforcement Fairness Act of 1996,[7] the Office of Management and Budget's (OMB's) Office of Information and Regulatory Affairs would be likely to determine that when finalized, this rule meets the criteria set forth in 5 U.S.C. 804(2) because it is projected to have an annualized effect on the economy of more than $100,000,000.

The Justification for this Rulemaking and Summary of Proposed Rule Provisions section at the beginning of this preamble contain a summary of this rule and describe the reasons it is needed. We present a detailed analysis below.

1. Summary of Costs and Benefits

The Department identified ten categories of quantifiable costs arising from these proposals that would apply to all regulated entities: (1) conducting a Security Rule compliance audit; (2) obtaining written verification from their business associates or subcontractors that the business associates or subcontractors, respectively, have conducted the required verification of compliance with technical safeguards; (3) notifying other regulated entities when workforce members' access to ePHI is terminated; (4) completing network segmentation; (5) disabling ports and removing extraneous software; (6) deploying MFA; (7) deploying penetration testing; (8) updating policies and procedures; (9) updating workforce training programs; and (10) revising business associate agreements. Additionally, group health plans would be required to update plan documents to require health plan sponsors' compliance with the administrative, physical, and technical safeguards according to the Security Rule and notification of group health plans when health plan sponsors activate their contingency plan. Business associates would have additional obligations to verify compliance with technical safeguards and provide it in writing to covered entities (and subcontractors to business associates) and to notify covered entities upon activation of their contingency plans. Finally, although plan sponsors are not directly subject to the HIPAA Rules, by virtue of the plan document requirements, the Department estimates that certain group

[7] Also referred to as the Congressional Review Act, 5 U.S.C. 801 et seq.

health plan sponsors (*e.g.*, employers that provide group health benefits) would likely incur some quantifiable costs to improve safeguards for their electronic information systems that affect the confidentiality, integrity, or availability of ePHI and to notify group health plans upon activation of plan sponsors' contingency plan.

The Department estimates that the first-year costs attributable to this proposed rule total approximately $9 billion. These costs are associated with regulated entities and health plan sponsors engaging in the regulatory actions described above. For years two through five, estimated annual costs of approximately $6 billion are attributable to costs of recurring compliance activities. Table 1 reports the present value and annualized estimates of the costs of this proposed rule covering a 5-year time horizon. Using a 2 percent discount rate, the Department estimates that this proposed rule would result in annualized costs of $6.8 billion for regulated entities and health plan sponsors combined.

Table 1. Accounting Table, Costs of the Proposed Rule, $ Billions[a]

Costs	Primary Estimate	Year Dollars	Discount Rate	Period Covered
Present Value	$34	2023	Undiscounted	2026-2030
Present Value	$32	2023	2%	2026-2030
Annualized	$7	2023	2%	2026-2030

[a] Figures are rounded.

As a result of the proposed changes in this NPRM, the enhanced security posture of regulated entities would likely reduce the number of breaches of ePHI and mitigate the effects of breaches that nonetheless occur. The Department has partially quantified these effects and presents them in a break-even analysis. The break-even analysis estimates that if the proposed changes in the NPRM reduce the number of individuals affected by breaches by 7 to 16 percent, the revised Security Rule would pay for itself. Alternatively, the same cost savings may be achieved by lowering the cost per affected individual's ePHI by 7 percent ($35) to 16 percent

($82), respectively.

The changes to the Security Rule would likely result in important benefits and some costs that the Department is unable to fully quantify at this time. As explained further below, unquantified benefits include reductions in reputational, financial, and legal harm from breaches of individuals' ePHI, reductions in disruptions to health care delivery, increased confidence among parties to health care business transactions, and improved quality of health care.

Table 2. Potential Non-quantified Benefits

Benefits[a]
Would benefit individuals by shielding them from unwanted disclosure of their ePHI and resulting reputational, financial, and legal harms from ePHI misuse.
Would reduce reputational damage to regulated entities resulting from breaches.
Would increase confidence among parties to health care business transactions that ePHI is protected to a higher degree than previously.
Would reduce risk of breaches of ePHI by health plan sponsors.
Would help to prevent health care cost increases to recoup financial losses from responding to breaches.
Would help guard against potential data loss.
Would help minimize potential disruption of service for individuals served by any of the affected entities.

[a] Some of the items in this list represent differing perspectives on the same effect. In such cases, if more thorough quantification became feasible, we would take steps to avoid double-counting when summing the quantitative estimates.

The Department also recognizes that there may be some costs that are not readily quantifiable, notably, actions that regulated entities may take to comply with existing requirements more fully as a result of proposed clarifications. For example, this would include completing a technology asset inventory, which is a baseline expectation for the existing requirement of conducting a risk assessment; documenting completion of existing requirements; adding more specificity to the required contingency plan, such as designating staff roles with specific responsibilities when a contingency occurs; testing safeguards as part of reviewing and updating policies and procedures and technical controls; and deploying encryption for ePHI in a more concerted manner (including documenting provision of notification in response to individuals' access requests for transmission of ePHI in an unencrypted manner and has been

informed of the risks associated with the transmission, receipt, and storage of unencrypted ePHI). These activities are specified in the NPRM, but they would be more in the nature of clarifications to and increased specificity of existing requirements. Because the degree of additional effort by regulated entities to meet these requirements would be dependent on multiple factors and likely to be highly variable, the additional cost is difficult to quantify.

We acknowledge that there may be a small burden associated with documenting that an individual was informed of the risks of unencrypted transmission of ePHI; however, we believe there are few requests that fall into this category. Because we do not have a basis to make an estimate, we have requested data on potential burdens associated with this proposed exception to the proposed standard for encryption in the preamble discussion of 45 CFR 164.312.

The cost of complying with the exceptions to encryption and MFA for medical devices authorized by the U.S. Food & Drug Administration for marketing may depend in part on the extent to which a regulated entity relies on legacy devices because the regulated entity may be required to adopt compensating controls. New devices are likely to have encryption and MFA built into them, not requiring compensating controls. The Department is unable to estimate the range of costs to adopt compensating controls for legacy devices because there is no reliable data to accurately assess the extent to which legacy devices are used in the United States.[8] The Department requests comment on the number of legacy devices in use and the costs of applying compensating controls to such devices.

2. Baseline Conditions

The Security Rule, in conjunction with the Privacy and Breach Notification Rules, protects the privacy and security of individuals' PHI, that is, individually identifiable health information (IIHI). The Security Rule's protections are limited to ePHI, while the Privacy and Breach Notification Rules protect both electronic and non-electronic PHI. The Security Rule establishes standards to protect individuals' ePHI and requires reasonable and appropriate

[8] "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks," *supra* note 742, p. 6.

administrative, physical, and technical safeguards. The Security Rule specifies a series of administrative, physical, and technical security requirements that must be performed or implemented for regulated entities to safeguard ePHI. Specifically, entities regulated by the Security Rule must: (1) ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain, or transmit; (2) protect against reasonably anticipated threats to the security and integrity of the information; (3) protect against reasonably anticipated impermissible uses or disclosures; and (4) ensure compliance by their workforce. A major goal of the Security Rule is protecting the security of individuals' health information while allowing for the development of a health information system to improve the efficiency and effectiveness of the health care system.

The Administrative Simplification provisions of HIPAA (title II) provide the Secretary of HHS with the authority to publish standards for the privacy and security of health information. The Department first proposed standards for the security of ePHI on August 12, 1998, and published a final rule on February 20, 2003. The Department modified the Security Rule in 2013. Recently, as the preamble to this NPRM discusses, changes in the health care environment and insufficient compliance by regulated entities with the existing Security Rule require the modifications proposed here.

For purposes of this Regulatory Impact Analysis (RIA), the proposed rule adopts the list of covered entities (with an updated count) and certain cost assumptions identified in the Department's Information Collection Request (ICR) associated with the HIPAA Privacy Rule to Support Reproductive Health Care Privacy ("2024 ICR").[910] The Department also relies on certain estimates and assumptions from the 1998 Proposed Rule[941] that remain relevant, the 2003 Final Rule,[11] and the 2013 Omnibus Rule,[943] as referenced in the analysis that follows.

---

[9] "View ICR," Office of Information and Regulatory Affairs, Office of Management and Budget (July 9, 2024), https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202401-0945-002.
[10] FR 43242 (Aug. 12, 1998).
[11] 68 FR 8334 (Feb. 20, 2003). [943]
78 FR 5566 (Jan. 25, 2013).

The Department quantitatively analyzes and monetizes the effect that this proposed rule would have on the actions of regulated entities to: conduct a Security Rule compliance audit; provide or obtain verification of business associates' compliance with technical safeguards; notify other regulated entities when workforce members' access to ePHI is altered or terminated; notify covered entities or business associates, as applicable, upon activation of a contingency plan; complete network segmentation; disable unused ports and remove extraneous software; deploy MFA and penetration testing; update health plan documents; update policies and procedures; update workforce training; and revise business associate agreements. The Department also quantitatively analyzes the effects on group health plan sponsors for ensuring that safeguards for their relevant electronic information systems meet Security Rule standards and notifying group health plans upon activation of the plan sponsors' contingency plans.

Additionally, the Department quantitatively analyzes the benefits of the proposed modifications to regulated entities due to an expected reduction in costs of remediation of breaches and risk of breaches by regulated entities.

The Department analyzes the remaining benefits and costs qualitatively because many of the proposed modifications are clarifications of existing requirements and predicting other concrete actions that such a diverse scope of regulated entities might take in response to this rule is inherently uncertain.

Analytic Assumptions

The Department bases its assumptions for calculating estimated costs and benefits on several publicly available datasets, including data from the U.S. Census Bureau ("Census"), the U.S. Department of Labor's (DOL) Bureau of Labor Statistics, the Small Business Administration (SBA), and the Department's Centers for Medicare & Medicaid Services (CMS) and Agency for Healthcare Research and Quality (AHRQ). For the purposes of this analysis, the Department assumes that employee benefits plus indirect costs equal approximately 100 percent of pre-tax wages and adjusts the hourly wage rates by multiplying by two, for a fully loaded

hourly wage rate. The Department adopts this as the estimate of the hourly value of time for changes in time use for on-the-job activities.

Implementing the proposals likely would require regulated entities to engage workforce members or consultants for certain activities. The Department assumes that an information security analyst would perform most of the activities proposed in the NPRM, consistent with the existing Security Rule requirements. The Department expects that a computer and information systems manager would revise policies and procedures, a training and development specialist would revise the necessary workforce training, a lawyer would revise business associate agreements, and a compensation and benefits manager would revise health plan documents for plan sponsors. To the extent that these assumptions affect the Department's estimate of costs, the Department solicits comment on its assumptions, particularly assumptions in which the Department identifies the level of workforce member (*e.g.*, analyst, manager, licensed professional) that would be engaged in activities and the amount of time that particular types of workforce members spend conducting activities related to this RIA as further described below. Table 3 lists pay rates for occupations referenced in the cost estimates for the NPRM.

Table 3. Occupational Pay Rates[12]

Occupation Code and Title	Fully Loaded Hourly Wage	2023 Average Hourly Wage
15-1212 Information Security Analysts	$119.94	$59.97
13-1151 Training and Development Specialists	$69.20	$34.60
11-3111 Compensation and Benefits Manager	$145.14	$72.57
11-3021 Computer and Information Systems Managers	$173.76	$86.88
23-1011 Lawyers	$169.68	$84.84
13-1111 Management Analysts	$111.08	$55.54
43-0000 Office and Administrative Support Occupations	$46.10	$23.05

[12] *See* "OCCUPATIONAL EMPLOYMENT AND WAGES – MAY 2023," U.S. Department of Labor, Bureau of Labor Statistics, Table 1. National employment and wage data from the Occupational Employment and Wage Statistics survey by occupation (Apr. 3, 2024), https://www.bls.gov/news.release/pdf/ocwage.pdf.

The Department assumes that most regulated entities would be able to incorporate changes to their workforce training into existing cybersecurity awareness training programs and Security Rule training rather than conduct a separate training because the total time frame for compliance from date of publication of a final rule would be 240 days.[13]

Regulated Entities Affected

The changes proposed in this NPRM would apply to covered entities (*i.e.*, health care providers that conduct covered electronic transactions, health plans, and health care clearinghouses) and their business associates (including subcontractors). The Department estimates the number of covered entities to be 822,600 business establishments (see table 4). By calculating costs for establishments, rather than firms,[14] some burdens may be overestimated because certain costs would be borne by a parent organization rather than each separate facility. Similarly, benefits and transfers would be overestimated because entity assumptions flow through to those quantifications. However, decisions about the level of an organization that is responsible for implementing certain requirements likely varies across the health care industry. The Department requests data on the extent to which certain burdens are borne by each facility versus an umbrella organization.

According to Census data,[15] there are 954 Direct Health and Medical Insurance Carrier firms out of a total 5,822 Insurance Carrier firms, such that health and medical insurance firms make up approximately 16.4 percent of insurance firms [= 954/5,822].[948] Also, according to Census data, there are 2,506 Third Party Administration of Insurance and Pension Funds firms and 8,375 establishments. This category also includes clearinghouses. The Department assumes that 16.4 percent of these firms service health and medical insurance because that is equivalent to the share of insurance firms that are health and medical. As a result, the Department estimates

[13] This includes 60 days from publication of a final rule to the effective date and an additional 180 days until the compliance date.
[14] A firm may be an umbrella organization that encompasses multiple establishments.
[15] "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," United States Census Bureau, U.S. & States, 6-digit NAICS (Dec. 2023), https://www.census.gov/data/tables/2021/econ/susb/2021-susb-annual.html. [948] This percentage was rounded.

that 411 firms categorized as Third Party Administrators are affected by the proposals in this NPRM [= 2,506 x .164]. Similarly, the Department estimates that 1,374 associated establishments would be affected by the proposals in this NPRM [= 8,375 total establishments x .164]. Most of these are business associates. Based on data from the Department's HIPAA audits and experience administering the HIPAA Rules, we are aware of approximately 36 clearinghouses. See table 4 below.

There were 56,289 community pharmacies, including 19,261 pharmacy and drug store firms, operating in the U.S. in 2023.[16] Small pharmacies generally use pharmacy services administration organizations (PSAOs) to provide administrative services, such as conducting negotiations. Based on information from industry, the Department estimates that the proposed rule would affect fewer than 10 PSAOs and we include this within the estimated 1 million business associates affected by the proposals in this NPRM.[17] The Department assumes that costs affecting pharmacies are incurred at each pharmacy and drug store establishment and each PSAO.

Table 4. Estimated Number, Type, and Size Threshold of Covered Entities

Covered Entities				
NAICS Code	**Type of Entity**	**Firms**	**Establishments**	**Small Business Administration (SBA) Size Threshold[c]**
524114	Health and Medical Insurance Carriers	954	5,552	$47 million
524292	Clearinghouses[a]	36	36	$47 million
622	Hospitals	3,095	7,465	$47 million
446110	Pharmacies[b]	31,671	56,289	$37.5 million

[16] *See* "2023 NCPA Digest, sponsored by Cardinal Health," National Community Pharmacists Association, Table 5, p. 9 (2023), https://www.cardinalhealth.com/content/dam/corp/web/documents/Report/cardinal-health-2023-ncpadigest.pdf; *see also* "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," *supra* note 947.

[17] *See* Scott Pace, "The Role and Value of Pharmacy Services Administrative Organizations (PSAOs)," Impact Management Group, p. 3 (July 20, 2022), https://content.naic.org/sites/default/files/call_materials/The%20Role%20and%20Value%20of%20Pharmacy%20Services%20Administrative%20July%202022.pdf; *see also* "The Role of Pharmacy Services Administrative Organizations for Independent Retail and Small Chain Pharmacies," Avalere Health, p. 4 (Sept. 30, 2021), https://documents.ncsl.org/wwwncsl/Foundation/sponsorviews/The_Role_of_PSAOs_Independent_Pharmacies.pdf.

6211-6213	Office of Drs. & Other Professionals	429,476	527,951	$9 - $16 million
6215	Medical Diagnostic Laboratories & Imaging	8,714	19,477	$19 - $41.5 million
6214	Outpatient Care	26,084	54,642	$19 - $47 million
6219	Other Ambulatory Care	10,547	16,114	$20.5 - $40 million
623	Skilled Nursing & Residential Facilities	42,421	95,175	$16 - $34 million
6216	Home Health Agencies	27,433	38,040	$19 million
532283	Home Health Equipment Rental	488	1,859	$41 million
Total		**580,919 8**	**822,600**	

[a] This North American Industry Classification System (NAICS) category includes clearinghouses and is titled "Third Party Administration of Insurance and Pension Funds." The number of clearinghouses is based on the Department's research. [b] Number of pharmacies is taken from industry statistics.

[c] *See* "Table of Small Business Size Standards," U.S. Small Business Administration (Mar. 17, 2023), https://www.sba.gov/sites/sbagov/files/2023-06/Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf. The SBA size thresholds are discussed in Section V.C. Regulatory Flexibility Act—Small Entity Analysis of this NPRM.

The Department also estimated the percentage of rural and urban health care providers by matching health care provider data from CMS,[18] Health Resources & Services Administration,[19] and the Statistics of U.S. Businesses (SUSB)[20] with county population data from the U.S. Census Bureau.[21] We determined whether a health care provider was rural or urban based on OMB's standards for delineating metropolitan and micropolitan statistical areas.[955] Consistent with OMB's standard, we considered a county to be rural if it has fewer than 50,000

[18] *See* "Provider of Services File - Internet Quality Improvement and Evaluation System - Home Health Agency, Ambulatory Surgical Center, and Hospice Providers," Centers for Medicare & Medicaid Services (2024), https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-internet-qualityimprovement-and-evaluation-system-home-health-agency-ambulatory-surgical-center-and-hospice-providers; "Provider of Services File - Hospital & Non-Hospital Facilities," Centers for Medicare & Medicaid Services (2024), https://data.cms.gov/provider-characteristics/hospitals-and-other-facilities/provider-of-services-file-hospital-nonhospital-facilities.

[19] *See* "Area Health Resources Files," Health Resources & Services Administration, U.S. Department of Health and Human Services (2022 - 2023 County Level Data), https://data.hrsa.gov/data/download?data=AHRF#AHRF.

[20] *See* "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," s*upra* note 947.

[21] *See* "Delineation Files," U.S. Census Bureau, U.S. Department of Commerce (2023), https://www.census.gov/geographies/reference-files/time-series/demo/metro-micro/delineation-files.html.

[955] *See generally* 86 FR 37770 (July 16, 2021). [956] *See* 86 FR 37770, 37778 (July 16, 2021).

inhabitants.[956] This includes micropolitan areas (towns and cities between 10,000 and 49,999) and counties outside of metropolitan statistical areas and micropolitan areas. Based on this analysis, we estimate that 7 – 8 percent of health care providers operate in rural areas.

Estimated Number and Type of Business Associates

The Department adopts the estimate of approximately 1,000,000 business associates (including subcontractors) as stated in the 2024 ICR and the 2013 "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health [HITECH] Act and the Genetic Information Nondiscrimination Act, and Other Modifications to the HIPAA Rules" final rule.[957] We considered whether to increase this figure in our updates but did not do so because many business associates serve multiple covered entities. We lack sufficient data to estimate the number of such businesses more precisely, but we believe that the number of business associates is highly dynamic and dependent on multiple market factors, including expansion and consolidation among various lines of business, changing laws and legal interpretations, and emerging technologies. We include subcontractors of business associates within our estimate because they are business associates of business associates.

The Department welcomes comments on the number or type(s) of regulated entities that would be affected by the proposals in this proposed rule and the extent to which they may experience costs or other burdens not already accounted for in the cost estimates. The Department also requests comment on the number of health plan documents that would need to be revised, if any. The Department additionally requests detailed comment on any situations, other than those identified here, in which covered entities or business associates would be affected by the proposals in this rulemaking.

Health Plan Sponsors

Within this NPRM, the Department is for the first time including estimates of health plan sponsors' potential costs of compliance with specific administrative, physical, and technical

safeguards of the Security Rule. The Department relied on data from AHRQ and the U.S. Census to estimate the number of firms offering group health plans (1.9 million),[958] and multiplied that by the percentage that offer at least one self-insured plan to calculate the number of plan sponsors that would be likely to receive ePHI and be subject to the requirements of 45 CFR 164.314(b) [1,943,484 x .382 = 742,411]. We solicit comments on whether group health plans or third-party administrators address any Security Rule requirements for plan sponsors, so the plan sponsors would not have an additional burden or would have a smaller burden than estimated below.

[957] 78 FR 5565 (Jan. 25, 2013).

[958] *See* "Medical Expenditure Panel Survey – Insurance Component," Tables I.A.1 and I.A.2, Agency for Healthcare Research and Quality (2023), https://meps.ahrq.gov/data_stats/summ_tables/insr/national/series_1/2023/ic23_ia_g.pdf?_gl=1*16xft35*_ga*MTE0MDI5NzI0LjE3MDk2NjQ0NDM.*_ga_45NDTD15CJ*MTczMTEwMzQ4OS4yLjEuMTczMTEwMzUzNS4xNC4wLjA (showing the number of establishments and percent offering health plans) and "County Business Patterns: 2021," United States Census Bureau (April 27, 2023), https://www.census.gov/data/datasets/2021/econ/cbp/2021cbp.html (providing the ratio of firms to establishments). We assume one health plan sponsor per firm that offers a self-insured group health plan.

Individuals Affected

The number of individuals potentially affected by the proposed changes to the Security Rule includes most of the United States population (approximately 337 million), specifically those who have received any health care in the past seven years and whose ePHI is likely created, received, maintained, or transmitted by a regulated entity. Statistics about the number of individuals affected by breaches of PHI provide insight into known instances where safeguards were breached, although the effects of the Security Rule extend farther than that, to all ePHI. Data from the 2022 Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022[22] revealed nearly 42 million individuals affected by breaches of PHI in that year. Third-party sources reported approximately 133 million individuals affected

[22] *See* "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022," *supra* note 213, p. 9 (2023).

by health care breaches in 2023.[23] According to UnitedHealth Group, the 2024 breach of its clearinghouse subsidiary Change Healthcare may have affected approximately one-third of the U.S. population, or 112 million individuals.[24] The Department believes that the range of individuals potentially affected by the proposed regulatory changes would be from 42 million to 337 million.

HIPAA Breach Data

The Department has reported HIPAA/HITECH breach data annually since 2009. Table 5 shows the data as reported to Congress for the past five years. We relied on this data, combined with breach cost data from industry sources, to analyze the potential savings of the NPRM.

Table 5. Breaches of PHI

Year	Small Breaches (fewer than 500 affected individuals)		Large Breaches (500+ affected individuals)		Total	
	Breach Count	Affected Individuals	Breach Count	Affected Individuals	Breach Count	Affected Individuals
2018	63,098	296,948	302	12,196,601	63,400	12,493,549
2019	62,771	284,812	408	38,732,966	63,179	39,017,778
2020	66,509	312,723	656	37,641,403	67,165	37,954,126
2021	63,571	319,215	609	37,182,558	64,180	37,501,773
2022	63,966	257,105	626	41,747,613	64,592	42,004,718

3. Costs of the Proposed Rule

Below, the Department provides the basis for its estimated quantifiable costs resulting from the proposed changes to specific provisions of the Security Rule. Many of the estimates are based on assumptions formed through OCR's experience with compliance and enforcement and accounts from stakeholders. For each cost, the Department provides its main estimate, as well as additional high and low estimates for some costs to account for any uncertainty in the compliance approach of regulated entities.

[23] *See* Steve Alder, "December 2023 Healthcare Data Breach Report," The HIPAA Journal (Jan. 18, 2024), https://www.hipaajournal.com/december-2023-healthcare-data-breach-report/.

[24] *See* "What We Learned: Change Healthcare Cyber Attack," U.S. House of Representatives Committee on Energy & Commerce (May 3, 2024), https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyberattack.

All estimates in this section are based on subject matter expertise. The Department requests information or data points from commenters to further refine its estimates and assumptions.

a. Costs Associated with Conducting a Security Rule Compliance Audit

The Department estimates that all regulated entities would need to conduct a Security Rule Compliance Audit because this would be a new requirement under proposed 45 CFR 164.308(a)(14). Although some regulated entities have mistakenly conducted such an audit in lieu of a risk analysis, the Department believes that costs for the compliance audit as a separate requirement should be attributed to the proposed changes in the NPRM. Further, because this would be an annual requirement, the Department is including this as a recurring cost. The Department estimates that regulated entities would need an average of 2 hours of labor by an information systems analyst to conduct the compliance audit, based on the assumption that regulated entities have already documented Security Rule compliance activities as currently required. This would result in total estimated costs of $437,205,288 [= 1,822,600 regulated entities x 2 hours x $119.94]. The respective low and high estimates would be 0.25 and 2.5 hours of information systems analyst labor, resulting in respective total estimated costs of $54,650,6611 [= 1,822,600 regulated entities x 0.25 hours x $119.94] and $546,506,610 [= 1,822,600 regulated entities x 2.5 hours x $119.94].

b. Estimated Costs from Adding a Requirement for Business Associates to Analyze Compliance with Technical Safeguards For

proposed 45 CFR 164.308(b), the Department estimates that business associates that handle ePHI would need to spend an average of 2 hours (with a low estimate of 0.25 hours and high estimate of 2.5 hours) analyzing how their cybersecurity measures comply with the proposed requirements for technical safeguards and producing a verification report for covered entities at the hourly wage rate of an information security analyst. This estimate assumes that business

associates have already documented existing safeguards, policies, and procedures, so that the costs attributable to the new requirement are incremental and would total approximately $239,880,000 [1 million business associates x 2 hours x $119.94], with a low estimate of $29,985,000 [1 million business associates x 0.25 hours x $119.94] and high estimate of $299,850,000 [1 million business associates x 2.5 hours x $119.94].

c. Costs Arising from Covered Entities and Business Associates Obtaining Verification from Business Associates of Compliance with Technical Safeguards

Under 45 CFR 164.308(b), the Department further estimates that each covered entity would need to spend an average of 30 minutes (with 15 minutes as a low estimate and 90 minutes as a high estimate) requesting and obtaining compliance reports from its business associates about their deployment of technical safeguards required by the Security Rule at the hourly wage of an information security analyst. This assumes that in most instances, business associates would produce the required verification for covered entities without being prompted by a request because they would be required to do so by the Security Rule, as proposed in the NPRM. It further assumes that covered entities have readily available means of contacting business associates, such as via email, and that the contact could be a single email draft sent in a batch. The average time burden per entity depends on verification frequency, likely influenced by entities' average number of business associates and how frequently entities change business associates. The low estimate assumes that entities verify less frequently, whereas the high estimate assumes entities verify more frequently. At the wage rate of an information security analyst, this would result in estimated total costs for covered entities of $49,331,322 [= 822,600 covered entities x 0.5 hours x $119.94], with a low estimate of $24,665,661 [= 822,600 covered entities x 0.25 hours x $119.94] and high estimate of $147,993,966 [= 822,600 covered entities x 1.5 hours x $119.94].

The proposed requirement to obtain verification of compliance with technical safeguards also would apply to business associates with respect to their subcontractors. However, we believe

that a much smaller number of business associates rely on subcontractors compared to the number of covered entities that rely on business associates to conduct activities on their behalf. Thus, we estimate that, on average, business associates would need 5 minutes annually to obtain verification from their subcontractors that the subcontractors have complied with technical safeguards as required by the Security Rule. The estimate includes only the time needed for business associates to send a mass email to subcontractors because we have already addressed the burden on business associates of producing the verification in the previous section and that estimate includes burdens on subcontractors. The high estimate for this activity would be an average of 15 minutes per business associate, and a low estimate would be for business associates to 2 minutes on this activity. At the wage rate of an information security analyst, this would add estimated total costs for business associates of $9,995,000 [= 1,000,000 business associates x 0.083 hours x $119.94], with a high estimate of $29,985,000 [= 1,000,000 business associates x .25 hours x $119.94].

d. Cost Related to Notification of Termination or Change of Workforce Members' Access to ePHI

The Department estimates that regulated entities are likely to incur additional costs to implement a process to notify other regulated entities when a workforce member's access to ePHI is terminated or changed under proposed 45 CFR 164.308(a)(9)(ii). This estimate assumes that notifications will take an average of 1 hour annually per regulated entity. This results in new estimated costs totaling $84,021,860 [= 1,822,600 regulated entities x 1 hour x $46.10].[25]

e. Cost Related to Regulated Entities Deploying Multi-Factor Authentication

The Department estimates that, on average, regulated entities would have an information security analyst spend 1.5 hours deploying MFA, as specifically required under proposed 45 CFR 164.312(f)(2)(ii). This would be a one-time, first-year burden that includes an average of 30

[25] *See* table 3, wage rate for Office and Administrative Support Occupations.

minutes for a regulated entity to select an MFA solution that allows them to meet the requirements of the proposal without creating workflow disruptions or delays. This estimate would vary depending on how prevalent MFA is in the industry when and if the requirements of the NPRM are finalized. As a widely accepted information security practice, the Department believes that many large entities have already deployed MFA and the costs range from zero to only a few dollars per user. The low estimate would be 01 hours on average (assuming that many entities already have some form of MFA), and the high estimate would be 1.75 hours (assuming that few entities have MFA). At the loaded wage rate of an information security analyst, the total estimated cost would be $327,903,966 [= 1,822,600 regulated entities x 1.5 hours x $119.94], with a low estimated total of $218,602,644 [= 1,822,600 regulated entities x 1 hour x $119.94] and a high estimated total of $382,554,627 [= 1,822,600 regulated entities x 1.75 hours x $119.94]. The Department applies this cost in the first year only because minimal additional labor is needed to maintain this safeguard once it has been deployed.

f. Costs Related to Network Segmentation

The Department believes that most large regulated entities and many medium-sized regulated entities have segmented their information networks to some degree; however, additional actions may be needed to more fully protect ePHI as required under proposed 45 CFR 164.312(a)(2)(vi). Further, small entities may not have been aware of the importance of segmenting networks or taken steps to segment their networks. The Department estimates that each regulated entity would spend an average of 4.5 hours to set up network segmentation in the first year of compliance with a final rule (with a low estimate of 4 hours and a high estimate of 5 hours) at the hourly wage of an information security analyst. The Department further assumes that in the following years, the burden to maintain the segmented network would be minimal and incorporated into the maintenance requirements. The total first year estimated cost of the network segmentation requirement would be $983,711,898 [= 1,822,600 regulated entities x 4.5 hours x $119.94] with a low estimated total of $874,410,576 [= 1,822,600 regulated entities x 4

hours x $119.94] and a high estimate of $1,093,013,220 [= 1,822,600 regulated entities x 5 hours x $119.94].

g. Cost Related to Disabling Ports and Removing Extraneous Software

The Department believes that large regulated entities have already disabled unused network ports and removed extraneous software as part of existing configuration requirements. However, the Department believes that small and medium-sized regulated entities are less likely to have performed these actions and thus would incur a new burden to implement these aspects of configuration management proposed at 45 CFR 164.312(c)(2)(ii) and (iv). The Department estimates that 629,796 establishments are owned by small and medium-sized covered entities,[26] which is approximately 76.56 percent of all covered entities [=629,796/822,600]. The Department applies that percentage to the estimated number of business associates [= 0.7656 x 1,000,000] to arrive at the estimated number of regulated entities with quantifiably increased burdens from these proposed requirements to disable unused ports and remove extraneous software. We estimate that for these 1,395,396 regulated entities [= 629,796 covered entities + 765,600 business associates], an average annual burden of 30 minutes would be needed at the wage rate of an information security analyst to make needed changes to configuration management, specifically disabling unused ports and removing extraneous software. This would result in estimated total cost increases of $83,681,898 [= 1,395,3960 regulated entities x 0.5 hours x $119.94], with a low estimate of $41,840,949 [= 1,395,396 regulated entities x 0.25 hours x $119.94] based on an estimated annual burden of 15 minutes per affected entity and a high estimate of $109,301,322 [= 1,822,600 regulated entities x 0.50 hours x $119.94] based on an estimated annual burden of 30 minutes for all regulated entities.

h. Costs Related to Regulated Entities Conducting Penetration Testing

[26] As defined by having 500 or fewer employees. *See* "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," *supra,* note 947 .

The Department estimates that each regulated entity would spend an average of 3 hours conducting penetration testing (with a low estimate of 2 hours and a high estimate of 10 hours) at the hourly wage of an information security analyst. The Department expects that there might be a high degree of variability between entities depending on their size and technological sophistication. Large entities have more endpoints to test, and thus have greater exposure. The Department also believes there is room for significant variability in the effort that regulated entities may apply to this activity. At the wage rate of an information security analyst, this would result in estimated total annual costs for regulated entities of $655,807,932 [= 1,822,600 regulated entities x 3 hours x $119.94], with a low estimated total of $437,205,288 [= 1,822,600 regulated entities x 2 hours x $119.94] and high estimated total of $2,186,026,440 [= 1,822,600 regulated entities x 10 hours x $119.94].

i. Costs Arising from Reporting Contingency Plan Activation The Department estimates that business associates would need to notify other regulated entities in the event that they activate their contingency plan once business associate agreements are revised according to proposed 45 CFR 164.314(a)(2)(i)(D). The Department believes this is unlikely to occur more frequently than once per year and that the time to do so would be minimal because the proposed requirement does not specify the means or scope of such notification. The Department estimates that business associates would need an average of 30 minutes (with 15 minutes as a low estimate and 45 minutes as a high estimate) to report to other regulated entities, as applicable, when their contingency plan is activated at the wage rate of an information security analyst for a total annual cost of $59,970,000 [= 1,000,000 business associates x 0.5 hours x $119.94], with a low estimated

total of $29,985,000[= 1,000,000 business associates x 0.25 hours x $119.94] and high estimated total of $89,955,000 [= 1,000,000 business associates x 0.75 hours x $119.94].

j. Revised Health Plan Documents

The Department estimates that health care insurers and third-party administrators would need to revise health plan documents to reflect that health plan sponsors that receive ePHI (that is not limited to summary health information or disenrollment information) are protecting ePHI with the administrative, physical, and technical safeguards detailed in the Security Rule, as proposed. These 6,162 entities collectively would be responsible for updating approximately 742,411 health plan documents at the wage rate of a compensation and benefits manager. The Department's estimate assumes that on average each plan document requires 30 minutes to update for a total estimated cost of $53,876,766 [1742,411 x 0.5 hours x $145.14]. The Department has attributed these costs solely to health plans and not health plan sponsors because the health plan is the regulated entity.

k. Estimated Costs for Developing New or Modified Policies and Procedures

The Department anticipates that regulated entities would need to develop new or modified policies and procedures for the proposed new requirements to obtain or provide verification of business associates' compliance with the Security Rule's requirements for technical safeguards, conducting a Security Rule compliance audit, and reporting the activation of a contingency plan, as well as other proposed changes, depending on the regulated entities' existing policies and procedures. The Department estimates that the costs associated with developing such policies and procedures would be the labor of a computer and information systems manager for an average of 3.5 hours (with 2.5 hours as a low estimate and 6 hours as a high estimate, depending on the number of entities with written policies and procedures, and their degree of specificity). This would result in total annual costs of $1,108,432,416 [= 1,822,600 regulated entities x 3.5 hours x $173.76], with a low estimated total of $791,737,440

[= 1,822,600 regulated entities x 2.5 hours x $173.76] and high estimated total of $1,900,169,856 [= 1,822,600 regulated entities x 6 hours x $173.76]. The existing rule requires updates to policies and procedures in response to environmental or operational changes affecting the security of the ePHI, and as a result, the Department is estimating additional costs for new policies related to this proposed rule as an incremental increase.

l. Costs Associated with Training Workforce Members The Department anticipates that regulated entities would be able to incorporate new content into existing Security Rule training programs and that the costs associated with doing so would be attributed to the labor of a training specialist for an estimated 2 hours for total annual costs of $252,247,840 [= 1,822,600 regulated entities x 2 hours x $69.20]. The low estimate for this activity is $126,123,920 [= 1,822,600 regulated entities x 1 hour x $69.20], and the high estimate is $378,371,760 [= 1,822,600 regulated entities x 3 hours x $69.20]. Many of the changes in the NPRM require the adoption of standard cybersecurity practices as applied specifically to address the confidentiality, integrity, and availability of ePHI, so we expect that an information security analyst would be familiar with this content. These estimated costs would address any required revisions to training for workforce members within the first year of compliance with a final rule. Any further recurring component is likely to be implemented into regularly scheduled employee training and thus would not be directly attributable to the proposals in this NPRM.

m. Revising Business Associate Agreements

The NPRM proposes to provide a transition period in proposed 45 CFR 164.318 for regulated entities to revise business associate agreements to comply with the proposed changes to the requirements of the Security Rule. The proposed transition period would allow regulated entities to revise existing agreements by the earlier of the contract renewal date that falls after the compliance date of a final rule, or within one year of the rule's effective date. For a large share of existing agreements, this would allow regulated entities to complete the revisions on a rolling basis according to the dates they are renewed. The Department estimates that 1,822,600[27] business associate agreements would need to be revised if this NPRM is adopted and that, on average, the portion of this activity that results from the rule's modifications would take an hour of a lawyer's time for each regulated entity. This would result in annual costs of $309,258,768 [= 1,822,600 regulated entities x 1 hour x $169.68]. The Department recognizes that this estimate may not fully account for all revised business associate agreements. However, the Department believes that in some instances, one hour of time is more than would be needed. We also believe it is likely that, for some regulated entities, a professional other than a lawyer would be responsible for the revised agreements at a lower hourly wage. For some large business associates, the Department believes that a single agreement is used for most of its customers. The Department's estimates assume that most agreements would be revised within the first year and accounts for all of them within that time period. This would be considered a one-time cost; in other words, it is not carried over into future years. As with all the estimates in this NPRM, the Department invites comments about the assumptions underlying the proposed cost projections.

n. Plan Sponsors' Obligations

Proposed 45 CFR 164.314(b)(2) would mandate that group health plan documents require their health plan sponsors who receive ePHI that is not limited to summary health information or enrollment or disenrollment information to deploy the administrative, physical, and technical safeguards for ePHI required by the Security Rule and notify their group health plans upon

[27] This is the estimated total number of covered entities and business associates.

activation of the plan sponsors' contingency plan. Currently, plan documents must require such health plan sponsors to have safeguards in place, but not necessarily the safeguards specified in the Security Rule.[28] The Department estimates that an additional 52.42 hours of labor would be needed for each affected health plan sponsor to bring its security safeguards for ePHI into compliance with the Security Rule standards and to notify group health plans when its contingency plan is activated, over and above the actions attributable to safeguards already in place for ePHI and for sponsors' electronic information systems generally. The Security Rule compliance activities attributed to group health plan sponsors are shown in table 7, below.

Most compliance activities would be performed by a workforce member at the hourly wage rate of an information security analyst ($119.94), while documentation of maintenance would be performed at the rate of a management analyst ($111.08) and notification of termination or change of workforce members' access to ePHI would be performed by an office administrative assistant ($46.10). This would result in estimated total first year costs for health plan sponsors of $4,658,781,219 as shown in detail in table 7.

o. Total Quantifiable Costs

The Department summarizes in tables 6 and 7 the estimated costs that regulated entities (approximately $4,655 million) and plan sponsors (approximately $4,659 million), respectively, would experience in the first year of implementing the proposed regulatory changes. The Department anticipates that these costs would be for the following activities: conducting a Security Rule compliance audit; obtaining verification of business associates' and subcontractors' compliance with technical safeguards; providing verification of business associates' compliance with technical safeguards; providing notification of termination or change of workforce members' access to ePHI; deploying MFA and penetration testing; segmenting networks; disabling unused ports; removing extraneous software; notifying covered entities or business associates, as applicable, upon activation of a contingency plan; and updating health

[28] *See* 45 CFR 164.314(b) (requiring that a group health plan ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan).

plan documents, policies and procedures, workforce training, and business associate agreements. These costs would also include health plan sponsors deploying safeguards for their relevant electronic information systems to meet Security Rule standards and notifying group health plans upon activation of a plan sponsor's contingency plan.

Table 6. First Year Cost Estimates for Regulated Entities' Proposed Compliance Obligations[a]

Compliance Activities	Burden Hours x Frequency	Respondents	Wage Rate	Total Annual Cost (millions)
Security Rule Compliance Audit	2 x 1	1,822,600 Regulated Entities	$119.94	$437
BA Verification of Technical Safeguards	2 x 1	1,000,000 Business Associates	$119.94	$240
Obtain BA Compliance Verification	.5 x 1	822,600 Covered Entities	$119.94	$49
Obtain Subcontractors' Compliance Verification	.083 x 1	1,000,000 Business Associates	$119.94	$10
Notification of Workforce Members' Termination of access to ePHI	1 x 1	1,822,600 Regulated Entities	$46.10	$84
Multi-factor Authentication	1.5 x 1	1,822,600 Regulated Entities	$119.94	$328
Network Segmentation	4.5 x 1	1,822,600 Regulated Entities	$119.94	$984
Configuration Management	.5 x 1	1,395,396 Regulated Entities	$119.94	$84
Penetration Testing	3 x 1	1,822,600 Regulated Entities	$119.94	$656
Notification of Contingency Plan Activation	.5 x 1	1,000,000 Business Associates	$119.94	$60

Update Health Plan Documents	.5 x 120	3,102,851 Health Plan Documents	$145.14	$54
Update Policies and Procedures	3.5 x 1	1,822,600 Regulated Entities	$173.76	$1,108
Update Workforce Training	2 x 1	1,822,600 Regulated Entities	$69.20	$252
Revise Business Associate Agreements	1 x 1	1,822,600 Regulated Entities	$169.68	$309
Total Annual Cost Burden				$4,655

[a] These represent first year estimated costs and are rounded.

The Department presents the estimated cost of health plan sponsors' compliance with the proposed new requirements in table 7 below.

Table 7. First Year Cost Estimates of Health Plan Sponsors' Proposed Compliance Obligations[a]

Compliance Activities	Burden Hours x Frequency	Respondents	Wage Rate	Total Annual Cost (millions)
Risk Analysis – Documentation	5 x 1	742,411 Plan Sponsors	$119.94	$445
Information System Activity Review - Documentation	.75 x 12	742,411Plan Sponsors	$119.94	$801
Ongoing Education	.17 x 12	742,411Plan Sponsors	$119.94	$178
Security Incidents (other than breaches) - Documentation	2 x 12	742,411 Plan Sponsors	$119.94	$2,137
Contingency Plan – Testing and Revision	2 x 1	742,411Plan Sponsors	$119.94	$178
Contingency Plan – Criticality Analysis	.5 x 1	742,411Plan Sponsors	$119.94	$45
Notification of Workforce Members' Termination of ePHI Access	.25 x 1	742,411Plan Sponsors	$46.10	$9
Maintenance Records	.5 x 12	742,411Plan Sponsors	$111.08	$495

Multi-factor Authentication	1.5 x 1	742,411Plan Sponsors	$119.94	$133
Configuration Management	.5 x 1	742,411 Plan Sponsors	$119.94	$45
Penetration Testing	2 x 1	742,411Plan Sponsors	$119.94	$178
Notification of Contingency Plan Activation	.17 x 1	742,411Plan Sponsors	$119.94	$15
Total Annual Cost Burden				$4,659

[a] These represent first year estimated costs and are rounded.

Together, regulated entities' and affected health plan sponsors' estimated first year costs of compliance with the proposals in the NPRM would be approximately 9,314 million (or $9 billion).

p. Costs Borne by the Department

The covered entities that are operated by the Department would be affected by the changes in a similar manner to other covered entities, and such costs have been factored into the estimates above. The Department has not identified other costs to the Department related to the changes in the NPRM. A reduction in the number of large breaches (affecting 500 or more individuals per incident) would benefit the Department by enabling it to focus its resources on a smaller number of breach investigations, and potentially resolve such investigations more quickly.

4. Benefits of the Proposed Rule

a. Quantitative Analysis of Benefits

A key goal of strengthening the cybersecurity posture of regulated entities is to reduce the number and severity of security incidents, including breaches of ePHI. The Department believes that compliance with the proposed changes, which align with industry guidelines and best practices, would benefit regulated entities by reducing the cost of breaches. Although the costs of implementing the proposed cybersecurity measures would be significant, the costs of responding

to breaches of ePHI are much higher. According to industry data, the average cost of a health care breach in 2023 rose to $10.93 million, the highest among all industries studied,[29] and the per record cost of a breach involving personally identifiable information (across all industries) was $183.[30] These costs include detection and investigation activities, notification activities, post-breach response activities, and activities attempting to minimize the loss of business. Thus, the benefits of the proposed rule would be to reduce the harms of health care breaches described in the preamble. The Department believes that implementing the changes in the NPRM would reduce both the incidence of breaches in health care and the costs of mitigating breaches when they occur.

The Department also analyzed the potential cost savings of proposals that correspond to major factors affecting the costs of large breaches as identified in published reports.[31] The Department estimates that, at a minimum, performing the following actions would quantifiably reduce costs: (1) encryption; (2) penetration testing; (3) requiring MFA and notification of termination of access to ePHI; (4) increasing employee training; and (5) reducing noncompliance with regulations. These factors would account for an estimated 23.6 percent decrease in large breach costs.[32] For health care breaches, this corresponds to an estimated cost savings of $2.6 million per large breach in high incidence years, and $2.1 million per large breach in low incidence years.

Non-quantitative Analysis of Benefits

A fundamental benefit of the proposed rule would be to decrease the effects of breaches on individuals who are the subjects of ePHI, namely patients and health plan members. Breaches of ePHI may cause harm to individuals in many ways, including loss of reputation and personal dignity and financial and medical fraud, which may result in false debts, impaired credit, and

---

[29] *See* "Cost of a Data Breach Report 2023," *supra* note 131, p. 13.
[30] *Id.* at 18.
[31] The impact factor costs and cost savings are based on estimates for all breaches from the annual IBM Security and Ponemon Institute Costs of a Data Breach Reports for years 2018 – 2023. *See id.* at p. 28.
[32] The Department calculated the percentage decrease as a share of the sum of factor costs from the average breach cost: ($218,915 + $180,358 + $187,703 + $221,593 + $232,867) / $4,450,000 = 0.236.

even health threats from misuse of health insurance credentials by another individual. "[H]ealthcare data, which includes medical histories and personal identification, can last a lifetime. The information collected can be used for ransom, to commit tax frauds, to provide supporting disability documentation, to send fake bills to insurance providers, to obtain healthcare, prescription drugs, medical treatment, and to obtain government benefits like Medicare and Medicaid."[33] Hackers can use stolen personal, medical, and financial data to take out a bank loan in the victim's name and change direct deposit information in payroll systems, allowing them to steal wages as well.[34] In addition, medical identity fraud can impact the victim's credit score and health insurance premiums, and may result in unexpected legal fees.[35] Medical identity fraud also enables thieves to obtain medical treatment using the victim's stolen ePHI. This can lead to the thief's medical conditions being incorporated into the victim's medical records and impacting the victim's ability to receive appropriate medical treatment based on accurate records in the future, or any care at all depending on whether the thief has exhausted the victim's insurance benefits.[36] Overall, recovering compromised ePHI and addressing the consequences of breached information can be a long and arduous process that can cost victims large amounts of time, energy, and money.[37]

Breaches of ePHI maintained by health care systems can also pose a threat to the medical well-being of affected individuals. Cyberattacks on health care organizations can include the deployment of malware that compromises the function of both internal and external medical devices. Such software can alter the dosages of sensitive medicines or shut down devices while

---

[33] *See* "New Dangers in the New World: Cyber Attacks in the Healthcare Industry," *supra* note 135, p. 3.
[34] *See* "Is the HIPAA Security Rule Enough to Protect Electronic Personal Health Information (PHI) in the Cyber Age?" *supra* note 207; *see also* Adam Wright, et al., "The Big Phish: Cyberattacks Against U.S. Healthcare Systems," Journal of General Internal Medicine, Volume 31, p. 1115-1118 (May 13, 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5023604/.
[35] *See* Thomas Clifford, "Provider Liability and Medical Identity Theft: Can I Get Your (Insurance) Number?," Northwestern Journal of Law & Social Policy, Volume 12, p. 45 (2016), https://scholarlycommons.law.northwestern.edu/njlsp/vol12/iss1/2/.
[36] *Id*.
[37] *Id*.

they are in use, thus affecting patient care.[38] Some of the medical devices that are vulnerable to malicious software attacks include insulin pumps and cardiac implant devices.[39] The consequences of a cyberattack on such a medical device can be fatal.

Cyberattacks on relevant electronic information systems also hinder the efficiency of hospitals and limit the quality of care provided to patients. Breaches of relevant electronic information systems negatively affect the routine functions of health care organizations. They can affect the availability of ePHI and relevant electronic information systems and redirect critical resources from patient care to addressing the cybersecurity attack. A 2020 cyberattack on a large covered entity disrupted communication and clinician access to medical records, including to individualized chemotherapy plan templates and tools for communicating during treatment preparation and delivery.[40] In the first week following the attack, the hospital's ability to provide critical outpatient care was reduced by 40 percent and infusion visit volume decreased by 52 percent. Many patients had to be transferred to other sites to minimize delays in receiving critical medications. The effects of this data breach are not unique to this provider. There is evidence that cyberattacks on health care organizations decrease the number of patients they are able to treat in a given day and staff utilization.[978] Decreases in efficiency and number of treated patients also cause health care facilities to lose revenue because of their inability to provide care during a cybersecurity event.

Similar to the effects of breaches of ePHI on individuals, health care organizations and facilities also experience reputational and financial impacts because of cybersecurity attacks.

---

[38] *See* "Assessing resilience of hospitals to cyberattack," *supra* note 130; *see also* Ashley Carman, "'MEDJACK' tactic allows cyber criminals to enter healthcare networks undetected," SC Media (June 4, 2015) ("Medjack" means a medical device hijack that attackers use to exploit outdated and unpatched medical devices), https://www.scmagazine.com/news/medjack-tactic-allows-cyber-criminals-to-enter-healthcare-networks-undetected.
[39] *See* "New Dangers in the New World: Cyber Attacks in the Healthcare Industry," *supra* note 135.
[40] *See* Steven Ades, et al., "Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect," JCO Oncology Practice, Volume 18, p. 23-24 (Aug. 2, 2021), https://pubmed.ncbi.nlm.nih.gov/34339260/. [978] *See* "Assessing resilience of hospitals to cyberattack," *supra* note 130.

Hospitals can lose the community's trust and be subject to lawsuits from individuals whose data was compromised.[41] Organizations that experience cybersecurity attacks can experience reputational harm and other monetary costs, such as those associated with providing breach notifications, paying fines to regulators and damages to individuals, and providing credit monitoring and identity theft-related services.[42] The harm to an organization's reputation is difficult to quantify, but it can also affect the quality of care administered to individuals.[43] Privacy and security of ePHI are paramount to individuals feeling safe and at ease sharing their IIHI with clinicians. Security breaches can negatively impact a patient's confidence in a health care organization if they believe their information and privacy may be compromised. This can cause them to delay seeking treatment or withhold information from health care practitioners, ultimately compromising the decision-making capacity of their health care provider to administer the best quality of care.[44] Decreasing the number and scope of health care breaches would reduce the harms of such breaches and would be a significant benefit of the proposals in the NPRM.

5. Comparison of Benefits and Costs

Key inputs to the estimation of costs of this proposed rule include the numbers of regulated entities and health plan sponsors. The Department has not previously quantified the costs of Security Rule compliance for health plan sponsors because the existing requirements are for plan documents to require such sponsors to implement administrative, physical, and technical safeguards, but not necessarily to comply with the specific requirements of the Security Rule. Therefore, the proposed requirement to comply with the proposed changes to the Security Rule, along with the number of affected plan sponsors (approximately 740,000), results in a significant

[41] *See* Mohammed Alkinoon, et al., "Measuring Health Care Data Breaches," Information Security Applications, Volume 13009, p. 265-277 (Aug. 11, 2021), https://dl.acm.org/doi/10.1007/978-3-030-89432-0_22.
[42] *See* "The Big Phish: Cyberattacks Against U.S. Healthcare Systems," *supra* note 971, p. 1115-1118.
[43] *See* "Health Records Database and Inherent Security Concerns: A Review of the Literature," *supra* note 177.
[44] *Id*.; *see also* Victoria Kisekka, et al., "The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes," Journal of Medical Internet Research, Volume 20 (Apr. 11, 2018), https://pubmed.ncbi.nlm.nih.gov/29643052/.

increase in overall cost estimates compared to the existing rule. The benefits of improved security for ePHI accrue to individuals, regulated entities, and health plan sponsors and are significant. The Department has discussed the benefits above.

The Department seeks to reduce the risk and mitigate the effects of breaches of ePHI and related information systems through the proposals included in this NPRM. Because the frequency and magnitude of cybersecurity events are inherently difficult to predict, we chose to conduct a break-even analysis in lieu of a cost savings analysis. The Department solicits comments with any information and data on the incidence and negative consequences of cybersecurity breaches.

The Department examined two different data points: the annual number of individuals affected by health care breaches, and the annual number of large breaches. Additionally, the Department considered a high and a low baseline based on the number of breaches and affected individuals per year. The Department calculated the high baseline as the average of the three highest values in the 6 years of available data (2018 to 2023, shown in table 8), and the low baseline as the average of the three lowest values.

Table 8. Data on Breaches of ePHI

Breach Years	**Affected Individuals for Large Breaches[a]**	**Cost[b] per Record[45]**
2018	12,493,549	$488
2019	38,732,966	$504
2020	37,641,403	$476
2021	37,182,558	$502
2022	41,747,613	$477
2023	113,173,613	$463
	# of Large Breaches (500+ individuals)	**Cost per Breach**
2018	302	$12,012,809
2019	408	$7,582,508
2020	656	$8,273,537

[45] For this analysis, a record is the ePHI of one individual.

2021	609	$10,241,897
2022	626	$10,468,138
2023	725	$10,930,000

[a] The numbers of affected individuals and numbers of large breaches are contained in the Reports to Congress on Breaches of Unsecured Protected Health Information for years 2018 – 2022, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reportscongress/index.html. Data for 2023 is contained in OCR's breach portal, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[b] The cost per record and cost per breach are based on estimates for health care breaches from the annual IBM Security and Ponemon Institute Costs of a Data Breach Reports for years 2018 – 2023. *See* "Cost of a Data Breach Report 2023," IBM Security, p. 10, 13 (July 24, 2023), *available at* https://www.ibm.com/reports/data-breach. Because only general breach costs were available for the 2020-2023 period, the Department adjusted those by multiplying them by the average of the ratios of health care-specific to overall breach costs for the years for which both data points were available (2018, $408/$148 and 2019, $429/$150). All dollar values were converted to 2023 dollars using the seasonally adjusted GDP Implicit Price Deflator, https://fred.stlouisfed.org/series/GDPDEF/.

The high baseline used 669 breaches and a total of 71 million individuals affected, and the low baseline used 440 breaches and 29 million individuals affected.[46] The high baseline represents years with higher incidence of breaches, whereas the low baseline represents years with lower incidence.

For each data point, the Department calculated the number of breaches or affected individuals by which the affected universe would have to decrease for the proposed rule to fully offset the annualized costs of regulated entities.[47] Table 9 and the discussion that follows analyses the costs and cost savings based on the number of individuals affected by breaches in a year and the cost per individual's ePHI or medical record.

Table 9. Break-Even Thresholds by Number of Affected Individuals

[46] *See* "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Year 2022," *supra* note 213, p. 9 (2023); "December 2023 Healthcare Data Breach Report," *supra* note 960.

[47] The break-even calculations presented here only include regulated entities because breach data is not available for health plan sponsors. Including sponsors and assuming they have the same rate of breaches would result in a similar break-even point in terms of percent decrease from baseline.

Baseline	Affected Individuals	Regulated Entities NPRM Costs	Unit Cost (per individual record)	Break-Even Threshold (NPRM Cost ÷ Unit Cost)	Percent Decrease (Threshold ÷ Affected) × 100
High	64,551,397	$2,251,258,305	$498	4,521,423	7%
Low	29,006,854				16.4%

The analysis in table 9 suggests that this NPRM would break even (cost savings would match monetized costs incurred) if the number of affected individuals is reduced by approximately 4.5 million. In years with a high incidence of breaches, this would be a reduction of approximately 7 percent, and in low-incidence years this would be a decrease of 16.4 percent. Thus, if the proposed changes in the NPRM reduce the number of affected individuals by 7 to 16 percent, the rule would pay for itself. Alternatively, the same cost savings may be achieved by lowering the cost per affected individual's ePHI by 7 percent ($35) and 16 percent ($82), respectively.

Table 10 analyzes the potential cost savings for regulated entities based on the annual number of large breaches of ePHI and the cost per breach, as shown below.

Table 10. Break-Even Thresholds by Number of Large Breaches

Baseline	Breaches	NPRM Cost for Regulated Entities	Unit Cost (per breach)	Break-Even Threshold (NPRM Cost ÷ Unit Cost)	Percent Decrease (Threshold ÷ Breaches) × 100
High	669	$2,251,258,305	$11,136,982	202	30.1%
Low	440				58.9%

In table 10, the Department assumes that the average cost per breach in industry reports ($11.1 million, calculated as the average of the three highest values in table 9, adjusted for inflation) refers to large breaches of ePHI . The analysis in table 10 suggests that the NPRM would break even if the annual number of large breaches is reduced by approximately 202. In high-incidence years, this would be a reduction of approximately 30 percent, and in lowincidence years, this would be a decrease of 59 percent. Alternatively, the same cost savings

may be achieved by lowering the cost per breach by 30 percent ($3.4 million) and 9 percent ($6.6 million), respectively.

B. Regulatory Alternatives To the Proposed Rule

The Department welcomes public comment on any benefits or drawbacks of the following alternatives it considered, but did not propose, while developing this proposed rule. We also request comment on whether the Department should reconsider any of the alternatives considered, and if so, why.

No Changes to the Security Rule

We considered not proposing revisions to the Security Rule. However, the Department believes that not revising the Security Rule would result in continued increases in both the number and size of breaches. Such increases would result in an exponential increase in costs as shown in table 8 above. If the modifications to the Security Rule result in even modest improvements to the security of ePHI, the reduction in the number and/or size of breaches would reduce the overall costs associated with breaches, including the costs of mitigating harm resulting from such breaches.

Email Security

The Department considered proposing a separate standard for regulated entities to secure email transmissions. In the Department's Cybersecurity Performance Goals,[48] the Department identifies email security as an essential goal for reducing risk from common email-based threats such as email spoofing, phishing, and fraud. Therein, the Department points to basic email protection controls identified in the Health Industry Cybersecurity Practices, such as spam/virus checking and real-time deny lists, as well as strategies that may be deployed across small, medium, and large organizations, including MFA for email access, email encryption, workforce education, and advance tooling (*e.g.*, URL click protection via analytics, attachment sandboxing).[49]

---

[48] "Cybersecurity Performance Goals," *supra* note 18.
[49] *Id*.

The Department is aware of the threat that email poses to the information systems of regulated entities and to the confidentiality, integrity, and availability of ePHI.[50] However, the Department believes that it is important that the Security Rule remain technology-neutral and that the security measures we propose in this NPRM apply to a regulated entity's information systems broadly, including email programs. For example, in this NPRM, the Department proposes to require regulated entities to encrypt all ePHI at rest and in transit and proposes a transmission security standard in which regulated entities would be required to deploy technical controls to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.[51] Therefore, the Department believes it is unnecessary to promulgate a separate standard for email security. Because the other technical controls, such as encryption and MFA, are already incorporated into the requirements that would protect relevant electronic information systems, the Department believes that adopting a separate secure email standard would duplicate costs without creating a net benefit.

Additionally, the Department considered whether to heighten the existing expectation[52] for regulated entities to inform individuals before transmitting ePHI to the individual via unencrypted email in response to a request for access under 45 CFR 164.524 by this means. We considered whether to require such notification for different types of requests, such as different categories of PHI (*e.g.*, billing, lab results, etc.), determining whether the individual had already received such notice, or providing notification upon each disclosure. Instead, the Department has proposed to clarify that notification must be provided for each request made by the individual under the individual right of access at 45 CFR 164.524 for their ePHI to be transmitted via

---

[50] According to the 2021 Verizon Data Breach Investigations Report, "phishing was 'present in 36% of breaches (up from 25% last year);' [and] 23% of malware was delivered through email." *See* "Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations," Cybersecurity Practice #1: Email Protection Systems, HHS Healthcare & Public Health Sector Coordinating Council, p. 13 (2023), https://405d.hhs.gov/Documents/tech-vol2-508.pdf (citing a 2021 Verizon Data Breach Investigations Report).

[51] *See* proposed 45 CFR 164.312(b)(2) and (g).

[52] *See* "Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524," What is the liability of a covered entity in responding to an individual's access request to send the individual's PHI to a third party?, Office for Civil Rights, U.S. Department of Health and Human Services, https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/access/index.html.

unsecure email. We believe that requiring a regulated entity to determine whether the individual had already received such notification would be more burdensome than incorporating the notification into the access request process, and instead, have proposed. We estimate that this could increase burdens for providing access via unsecure means by approximately one minute per request of this type. We lack data to estimate the number of requests for access via unsecure means.

Small and Rural Health Care Providers

Consistent with the requirement that the Secretary adopt security standards that take into account the needs and capabilities of small health care providers and rural health care providers,[53] the Department considered excepting small and rural health care providers from the requirement to perform penetration testing at proposed 45 CFR 164.308(h)(2)(iii) to lower anticipated costs of the rule for such providers. The Department estimates that approximately 90 percent of providers are small (based on revenue). Thus, the estimated cost reduction from this exemption (as compared to the proposed requirement for all regulated entities), would be approximately $266,389,139 [822,600 x .9 x 3 hours x $119.94 wage of an information security analyst] annually. While the Department is aware of the cost implications of this requirement for small and rural health care providers, we also believe that penetration testing is a critical component of managing vulnerability to cyberthreats across the health care sector. Additionally, we believe that setting different requirements for cybersecurity for small and rural health care providers would lead such health care providers to believe that they can limit their investment in cybersecurity. Given that a significant amount of health care is provided by small and rural health care providers, limiting their investment in cybersecurity would create a sizable gap in security protections. Such a gap has the potential to increase such providers' attractiveness to cybercriminals.

[53] 42 U.S.C. 1320d–2(d)(1)(A)(v).

The Department also considered proposing to permit small and rural health care providers to adopt alternate compensating controls, in lieu of the specified implementation specifications, to meet certain standards. After careful consideration, the Department concluded that it potentially could be just as costly to identify and adopt compensating controls that are reasonable and appropriate for small and rural health care practices. Small and rural health care providers would likely need to either hire personnel or contract with cybersecurity experts to identify potential compensating controls that would meet the relevant standard and provide implementation support. Accordingly, the Department declines to put forward such proposals at this time.

The Federal Information Security Modernization Act

The Department considered the requirements of the Federal Information Security Modernization Act (FISMA)[54] and whether compliance with FISMA by Federal agencies that are also regulated entities would be comparable to meeting the proposals in this NPRM. FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[993] After careful consideration, the Department does not believe that a regulated entity's compliance with FISMA would necessarily ensure compliance with all applicable proposed requirements in this NPRM because FISMA's requirements and the Security Rule's requirements are designed to serve different purposes. FISMA primarily focuses on securing Federal information systems, while the Security Rule applies specifically to ePHI. This NPRM contains specific proposed requirements, not found in FISMA, which are tailored to ensure the confidentiality, integrity, and availability of ePHI. Therefore, although the Department believes that FISMA requirements are consistent with those in the Security Rule and the proposals in this NPRM, we decline to propose that compliance with FISMA requirements

[54] Pub. L. 113-283 (Dec. 18, 2014) (codified at 44 U.S.C. 3551 *et seq*.). [993] *Id*.

would be a comparable alternative to compliance with the proposals in this NPRM. Instead, we believe that FISMA requirements complement the Security Rule and the proposed requirements and will facilitate the ability of regulated entities that are also subject to FISMA to fulfill their compliance with the HIPAA Rules.

Modifications to the Definition of "Information System"

The Department considered proposing additional modifications to the definition of "information system." The Security Rule currently defines the term "information system" as an interconnected set of information resources under the same direct management control that shares common functionality and includes hardware, software, information, data, applications, communications, and people.[55] This definition is based on the definition of "general support system" or "system" in the appendix to the 1996 version of OMB Circular A-130, Security of Federal Automated Information Systems.[56] We considered proposing to remove the phrase "under the same direct management control" as a potential way to clarify the application of the definition to cloud-based computing. Cloud computing applications play an important role in health care today. For example, many health care providers have implemented cloud-based electronic health records (EHRs) and practice management systems. These applications are used to create, receive, maintain, and transmit ePHI, and as such, should be included as components of a covered entity's relevant electronic information system, a term which is based upon the term "information system." After careful consideration, we have decided to retain the phrase "under the same direct management control" and instead clarify in the preamble how the definition of "information system" applies in cloud computing environments. The Department also requests comment on the definition of "information system" and the extent of control a regulated entity has with respect to applications in cloud computing environments.

---

[55] 45 CFR 164.304 (definition of "Information system").

[56] "Managing Information as a Strategic Resource," Circular No. A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, Office of Management and Budget, Executive Office of the President (Feb. 8, 1996), https://georgewbushwhitehouse.archives.gov/omb/circulars/a130/a130.html.

We also considered proposing to adopt the definition of "information system" in the Paperwork Reduction Act of 1995 (PRA) and the current operative version of OMB Circular A130.[57] The PRA and OMB Circular A-130 define "information system" as "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." The Department declined to adopt this definition because the existing definition in the Security Rule based on the definition of "system" in the 1996 version of OMB Circular A-130 more accurately reflects the typical components of an information system and the full extent of resources that are addressed by the Security Rule. Additionally, the definition of "information system" in the PRA and current operative version of OMB Circular A-130 contains some terms that are defined by the HIPAA Rules and some that are not. As a result, adopting this definition would require the Department to propose definitions to such additional terms and to ensure that the manner in which the terms with existing definitions are used is consistent with those existing definitions, and we are concerned that such change could cause significant confusion for regulated entities.

We do not believe that either of the alternative definitions considered would have generated a quantifiable change in costs because the alternatives would be clarifications to existing requirements and would not have changed the scope of the Security Rule's applicability.

Exception from Multi-factor Authentication (MFA) Requirement

The Department considered proposing an exception to the MFA authentication requirement that would permit regulated entities in the future to adopt other technologies, in lieu of MFA, that might offer a more secure method of authenticating user identity.[997] Based on discussions with cybersecurity experts, the Department believes that MFA is likely to remain the most secure method for authenticating user identity in future years. It may take different forms,

---

[57] Pub. L. 104–13, 109 Stat. 166 (May 22, 1995) (codified at 44 U.S.C. 3502(8)) (definition of "information system"); *see also* "Managing Information as a Strategic Resource," Circular No. A-130, Office of Management and Budget, Executive Office of the President, p. 31 (Jul. 28, 2016), (definition of "information system") https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf. [997] Proposed 45 CFR 164.312(f)(2)(ii).

but it will still, at its core, meet the definition of MFA proposed in this NPRM for the foreseeable future.[58]

While the Department acknowledges that technology will continue to evolve, we are unable to predict when and whether future technology will address identity verification and exceed the level of protection offered by MFA. This uncertainty renders us unable to articulate requirements specific enough to justify a purposeful exception. Because of the uncertainty surrounding new technologies, we are also unable to estimate costs of adopting this alternative. Our current view is that proposing and codifying such an exception would be premature, but we will revisit the proposed specific requirement for MFA, if adopted, and reconsider the need for an exception should a more secure technology emerge.

Transition for Business Associates and Group Health Plans

The Department considered requiring regulated entities to comply with all of the proposals in this NPRM by the compliance date, rather than proposing transition provisions for existing business associate agreements or other contractual arrangements. Had the Department taken that approach, we would have proposed that regulated entities update all existing business associate agreements by the proposed compliance date to comply with all applicable proposed requirements in this NPRM. While the Department believes that many of the proposals in this NPRM are consistent with the Security Rule as it currently exists, we are also concerned that too many regulated entities are not currently compliant with the Security Rule. Given the demonstrable increase in breaches, we believe that it is more important for regulated entities to first improve their cybersecurity posture by coming into compliance with all applicable proposed requirements in this NPRM, if adopted. Upon doing so, the Department anticipates that regulated entities will be better positioned to evaluate their contractual needs and to modify existing business associate agreements. For this reason, the Department has proposed the transition provisions in proposed 45 CFR 164.318. Not allowing for a transition period could have an

[58] 45 CFR 164.304 (proposed definition of "Multi-factor authentication").

opportunity cost whereby regulated entities spend their limited time revising business associate agreements instead of enhancing their cybersecurity posture. The Department believes that this could result in duplicative costs because some regulated entities may identify the need for additional changes to business associate agreements after they have fully evaluated their changed cybersecurity needs. The Department estimates that small regulated entities may be more likely to experience that outcome without a transition period, and thus the alternative of no transition period would cause a potential one-time increase in costs of $278,332,891 [(1,822,600 regulated entities x .9) x 1 hour x $169.68 lawyer hourly wage].

Relatedly, the Department considered proposing similar transition provisions for group health plans and plan sponsors that would provide these entities with additional time to update plan documents to align with new proposed requirements in this NPRM, if adopted. However, the Department believes that affected plans and plan sponsors would be able to complete any necessary updates by the proposed compliance date. The Department believes that updating plan documents is not as complex a task as evaluating potential new contractual needs to meet business associate obligations. Additionally, plan sponsors do not have Security Rule obligations independent of plan documents, and thus would not be obligated to implement the requirements proposed in this NPRM absent updates to the plan documents. The result of a transition period for updating plan documents would be merely to delay compliance with the changed Security Rule requirements, and therefore, delay improvements to their cybersecurity posture, not to reduce costs. Accordingly, we are not proposing such transition provisions in this NPRM.

C. Regulatory Flexibility Act—Small Entity Analysis

The Department has examined the economic implications of this proposed rule as required by the RFA. If a rule has a significant economic impact on a substantial number of small entities, the RFA requires agencies to analyze regulatory options that would reduce the economic effect of the rule on small entities. As discussed in greater detail below, this analysis concludes,

and the Secretary proposes to certify, that the proposed rule, if finalized, would not result in a significant economic effect on a substantial number of small entities.

For purposes of the RFA, small entities include small businesses, nonprofit organizations, and small governmental jurisdictions. The Act defines "small entities" as (1) a proprietary firm meeting the size standards of the SBA, (2) a nonprofit organization that is not dominant in its field, and (3) a small government jurisdiction of less than 50,000 population. The Department has determined that roughly 90 percent or more of all health care providers meet the SBA size standard for a small business as shown in table 4 or are a nonprofit organization. Therefore, the Department estimates that there would be 740,348 small entities affected by the proposals in this proposed rule.[59] The SBA size standard for health care providers ranges between a maximum of $9 million and $47 million in annual receipts, depending upon the type of entity, as shown in table 4, above.[60][61]

With respect to health insurers, the SBA size standard is a maximum of $47 million in annual receipts, and for pharmacy benefits and clearinghouses it is $45.5 million.[62] While some insurers are classified as nonprofit, it is possible they are dominant in their market. For example, a number of Blue Cross/Blue Shield insurers are organized as nonprofit entities; and yet, they dominate the health insurance market in the States where they are licensed.[63]

With respect to business associates, they provide a wide range of services for covered entities, including computer infrastructure, clearinghouse activities, leased office equipment, and professional services, such as legal, accounting, business planning, and marketing. The SBA size

---

[59] 740,348 = 822,609 covered entities x .90.

[60] *See* "Table of Small Business Size Standards," U.S. Small Business Administration (Mar. 17, 2023), https://www.sba.gov/sites/sbagov/files/2023-

[61] /Table%20of%20Size%20Standards_Effective%20March%2017%2C%202023%20%282%29.pdf.

[62] *Id*.

[63] "Market Share and Enrollment of Largest Three Insurers – Large Group Market," Kaiser Family Foundation (2019), https://www.kff.org/other/state-indicator/market-share-and-enrollment-of-largest-three-insurers-large-groupmarket/?currentTimeframe=0&sortModel=%7B%22colId%22:%22Location%22,%22sort%22:%22asc%22%7D.

thresholds for these industries ranges from $15.5 million for lawyers to $47 million for clearinghouses.[64]

For the reasons stated below, the Department does not expect that the cost of compliance would be significant for small entities. Nor does the Department expect that the cost of compliance would fall disproportionately on small entities. Although many of the regulated entities affected by the proposals in this proposed rule are small entities, they would not bear a disproportionate cost burden compared to the other entities subject to the rule. The projected total costs are discussed in detail in the RIA. The Department does not view this as a substantial burden because the result of the changes would be annualized costs per regulated entity of approximately $1,235 [= $2.3 billion[65]/1,822,600 regulated entities]. The per-entity costs represent the costs per establishment. As a result, smaller entities' costs are lower because they have fewer establishments. Larger regulated entities (*i.e.*, firms) that have multiple facilities (*i.e.*, establishments) would experience higher costs than the average cost per establishment because each firm would need to apply the proposals to all of their establishments. In the context of the RFA, HHS generally considers an economic impact exceeding 3 percent of annual revenue to be significant, and 5 percent or more of the affected small entities within an identified industry to represent a substantial number.

More than 5 percent of the small covered entities listed under the NAICS codes in table 4 are one-establishment firms with fewer than five employees,[66] so the analysis must determine how the effects of the quantified costs on one-establishment firms compare to their revenues. As

---

[64] *See* "Table of Small Business Size Standards," *supra* note 1000.

[65] This figure is rounded and represents annualized costs discounted at a 2 percent rate. The actual figure is $2,251,258,305.

[66] SUSB 2017 reports average revenue per firm by employment size. The size categories begin with less than 5 employees followed by 5 to 10 employees, and so on, with the largest categories representing firms with 2,500 to 4,999 employees and 5,000 or more employees). "2017 [Statistics of U.S. Businesses] Annual Data Tables by Establishment Industry," (May 2021), https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html. We inflated these revenues to 2021 dollars using the GDP deflator to estimate average revenues in each employment class in 2021 because that is the latest year for which data is reported. *See* "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," *supra* note 947. We then concluded that more than 5 percent of the firms whose revenues fall below the SBA thresholds (see table 4) belong to the "fewer than 5 employees" category and operate a single establishment.

explained above, the cost for a one-establishment firm is $1,235, so only small firms whose revenues are below $41,167 [=$1,235/0.03] would experience an effect exceeding 3 percent.

Among the NAICS codes for health care providers, the small firms with the lowest revenues are one-establishment HMO [Health Maintenance Organization] Medical Centers (NAICS 621491) with fewer than five employees, which had an estimated average yearly revenue in 2021 of $108,000. Residential Intellectual and Developmental Disability Facilities (NAICS 623210) had the second lowest revenues for one-establishment firms with fewer than five employees, with $180,000. Offices of Mental Health Practitioners (NAICS 621330) have the third lowest revenues for one-establishment firms with fewer than five employees, with $189,000. Thus, the Department believes that almost all regulated entities have annual revenues that exceed these amounts.

The Department acknowledges that there may be very small firms—namely firms without employees—whose revenues are below $41,167. We believe that such firms would comply with the regulation by purchasing services from software and web-hosting companies whose costs may increase as a result of the proposed changes. Such software and web-hosting companies would be business associates, and thus costs to them are already accounted for. We believe that, to the extent that these business associates decide to recover their minor cost increases by raising the prices of the services sold to non-employer firms, these incremental costs passed through to their small-firm customers would be negligible because they will be spread among many non-employer firms.

The Department has separately analyzed the effects of the NPRM on health plan sponsors and does not view the projected costs as a significant burden because the proposed changes would result in annualized costs per plan sponsor of approximately $6,133 [=$4,552,995,816 /742,411 health plan sponsors]. The quantified impact of $6,133 per health plan sponsor would only apply to those sponsors whose annual revenue is $204,433 or less.[67] The Department

[67] $6,133 is 3 percent of $204,433.

believes there are few, if any, group health plan sponsors with annual revenues below this amount because the average revenue of a U.S. business with 1 – 4 employees is $387,000[68] and employers with 0 – 1 employees are unlikely to sponsor a group health plan.

Accordingly, the Department believes that this proposed rule, if adopted, would be unlikely to affect a substantial number of small entities that meet the RFA threshold. Thus, this analysis concludes, and the Secretary proposes to certify, that the NPRM would not result in a significant economic effect on a substantial number of small entities.

HIPAA requires the Department to consider the needs and capabilities of small and rural health care providers.[69] As we explained in our 2003 analysis of the effect of the Security Rule on small and rural health care providers, the scalability provisions preclude the need to precisely define those categories.[70] We have long considered the effect of our rules on small businesses in the Small Entity Analysis discussed above. However, because of the breadth of changes proposed in this NPRM, the Department has considered more closely how it would affect rural health care providers. There are approximately 2,000 rural hospitals,[71] comprising nearly 30 percent of all hospitals [= 2,057/7,465],[1011] and the Department estimates approximately 7 to 8 percent of all health care providers operate in rural areas (counties or micropolitan areas with fewer than 50,000 inhabitants). See Regulated Entities Affected in Section V.A.2. Baseline Conditions, above.

Because rural health care providers are more likely to be small businesses, they would be affected in a manner similar to small entities, as demonstrated in the Small Entity Analysis above. Likewise, to the extent that Tribal health care providers are in rural areas, which many

---

[68] "Average Small Business Revenue: What To Know," Fora Financial (Jan. 11, 2023), https://www.forafinancial.com/blog/small-business/average-small-business-revenue/.
[69] 42 U.S.C. 1320d–2(d).
[70] *See* 68 FR 8334, 8341 (Feb. 20, 2003).
[71] *See* "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," *supra* note 306. *See also* table 4 above, SBA size threshold for hospitals. [1011] *See* "2021 [Statistics of U.S. Businesses] SUSB Annual Data Tables by Establishment Industry," *supra* note 947 (count of hospitals).

are,[72] our analysis of the effects on rural health care providers generally also applies. However, Tribal health providers have the benefit of access to centralized supportive services for health IT and EHR adoption, which other rural providers may lack.[73] A primary barrier to both adoption of health information technology (health IT) and deployment of cybersecurity safeguards in rural communities is limited access to high-speed internet. Rural health care providers, such as hospitals, have adopted EHRs at a lower rate than non-rural hospitals,[74] and thus may also have fewer electronic information systems that are subject to the Security Rule requirements, which could ease some burdens of compliance. However, as EHR adoption has increased in rural hospitals,[75] so too have the risks of cybersecurity attacks.[76] Rural health care providers are more likely to have limited resources to update legacy information technology (IT) systems, implement new or changed regulatory requirements, and respond to large breaches. Additionally, the health IT workforce is more limited in rural areas, which may affect the ability of rural health care providers to access in-person technical assistance. Because most rural hospitals are "located more than 35 miles from another hospital," responding to cyberattacks may be more challenging.[77] We request comment on the burdens these proposals would impose on rural health care providers, including rural hospitals.

Rural health care providers and other regulated entities can avail themselves of grants and incentives to improve broadband access and adoption of health IT.[78] For cybersecurity in

---

[72] The Indian Health Service funds a "network of over 600 hospitals, clinics, and health stations on or near Indian reservations in service areas that are rural, isolated, and underserved." "Justification of Estimates for Appropriations Committees, Fiscal Year 2025" Indian Health Service, U.S. Department of Health and Human Services, p. CJ-39 (Mar. 5, 2024).

[73] *See id.* at p. CJ-63–75.

[74] *See* "Telehealth and Health Information Technology in Rural Healthcare," Rural Health Information Hub, https://www.ruralhealthinfo.org/topics/telehealth-health-it#challenges-for-rural-communities.

[75] *See* "Percent of Hospitals, By Type, that Possess Certified Health IT," *supra* note 298.

[76] Kat Jercich, "Rural hospitals are more vulnerable to cyberattacks – here's how they can protect themselves," *supra* note 295.

[77] *See* "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," s*upra* note 306.

[78] Hannah Neprash, et al., "What happens to rural hospitals during a ransomware attack? Evidence from Medicare data," The Journal of Rural Health (Mar. 17, 2024), https://pubmed.ncbi.nlm.nih.gov/38494590/. For information about grants and incentives available for improving broadband access and adoption of health IT, *see, e.g.*, "Funding

particular, the White House, in partnership with private companies, announced the availability of direct assistance to rural health care providers on cybersecurity in the form of grants, discounts, and technical advice.[79] Additionally, CISA has compiled a list of free services and tools available to regulated entities from private and public sector entities. CISA also has published, in partnership with the Joint Cyber Defense Collaborative, a list of cybersecurity resources especially focused on high-risk communities.[80] And the Advanced Research Projects Agency for Health announced plans to invest $50 million to develop an autonomous solution for addressing cyberthreats to assist hospitals in defending their information systems.[81]

Cybersecurity is as essential for small and rural health care providers and their business associates, as it is for large and urban regulated entities. The seamless flow of data and increased connectivity means that threats to one health care provider do not affect only that one health care provider, regardless of size or location. The effects on patient care may be greater in rural environments where fewer alternatives exist if care is delayed or denied as a result of a cyberattack or malfunction.[82] As discussed in the preamble, the factors described at 45 CFR 164.306(b)(2) provide the flexibility for small and rural providers, in particular, to adopt security measures that are reasonable and appropriate for their circumstances.

D. Executive Order 13132—Federalism

As required by E.O. 13132 on Federalism,[1023] the Department has examined the provisions in the proposed regulation for their effects on the relationship between the Federal Government and the States. E.O. 13132 establishes certain requirements that an agency must

---

Programs," BroadbandUSA, National Telecommunications and Information Administration, U.S. Department of Commerce, https://broadbandusa.ntia.doc.gov/funding-programs; "Rural Health Care Program," Federal Communications Commission, https://www.fcc.gov/general/rural-health-care-program.

[79] *See* "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," s*upra* note 306.

[80] *See, e.g.*, "Free Cybersecurity Services and Tools," *supra* note 313; "Cybersecurity Resources for High-Risk Communities," *supra* note 313.

[81] *See* "Fact Sheet: Biden-Harris Administration Bolsters Protections for Americans' Access to Healthcare Through Strengthening Cybersecurity," s*upra* note 306; *see also* "UPGRADE, Universal Patching and Remediation for Autonomous Defense," Advanced Research Projects Agency for Health (May 20, 2024), https://arpah.gov/research-and-funding/programs/upgrade.

[82] "What happens to rural hospitals during a ransomware attack? Evidence from Medicare data," s*upra* note 1018.

[1023] 64 FR 43255 (Aug. 4, 1999).

meet when it promulgates a proposed rule (and subsequent final rule) that imposes substantial direct requirement costs on State and local governments, preempts State law, or otherwise has federalism implications. In the Department's view, the proposed rule would not have any federalism implications.

The federalism implications of the Security Rule were also assessed as required by E.O. 13132 and published as part of the preambles to the final rules on February 20, 2003[83] and January 25, 2013.[84] Regarding preemption, HIPAA dictates the relationship between State law and HIPAA regulatory requirements.[85] The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) provides that the HIPAA preemption provisions shall apply to the HITECH Act provisions and requirements.[86] As explained by the House report that accompanied the American Recovery and Reinvestment Act of 2009, the HITECH Act would not only apply HIPAA's preemption provisions to the HITECH Act requirements, but it would also "preserve the HIPAA privacy and security standards to the extent that they are consistent with" the HITECH Act.[87]

A requirement, standard, or implementation specification adopted in accordance with HIPAA and the HIPAA Rules supersedes any contrary provision of State law, subject to certain exceptions.[88] Specifically, State law would be preempted under the Security Rule only when (1) a regulated entity finds it impossible to comply with both State and Federal requirements; or (2) the provision of State law stands as an obstacle to accomplishing and executing the purposes and objectives of the Administrative Simplification provisions or the HITECH Act.[89] Although a

---

[83] 68 FR 8334, 8373 (Feb. 20, 2003).
[84] 78 FR 5566, 5686 (Jan. 25, 2013).
[85] 42 U.S.C. 1320d–7.
[86] Sec. 13421(a) of the HITECH Act; *see also* 45 CFR part 160, subpart B.
[87] *See* "MAKING SUPPLEMENTAL APPROPRIATIONS FOR JOB PRESERVATION AND CREATION, INFRASTRUCTURE INVESTMENT, ENERGY EFFICIENCY AND SCIENCE, ASSISTANCE TO THE UNEMPLOYED, AND STATE AND LOCAL FISCAL STABILIZATION, FOR THE FISCAL YEAR ENDING SEPTEMBER 30, 2009, AND FOR OTHER PURPOSES," Conf. Report to Accompany H.R. 1, p. 502 (Feb. 12, 2009).
[88] 42 U.S.C. 1320d–7(a); 45 CFR 160.203.
[89] *See* 45 CFR 160.202 (definition of "Contrary"). Preemption also applies if the provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives and purposes of sec. 264 of

few States (*e.g.*, California and New York) have promulgated or are in the process of promulgating regulations pertaining to cybersecurity in health care that may be more stringent than the Security Rule, the Department believes that a regulated entity could comply with both sets of requirements by adhering to the more stringent standard. Thus, in such cases, the State law would not be an obstacle to the accomplishment and execution of HIPAA or the HITECH Act.

The proposed modifications to the Security Rule would further the Congressional intent to improve the Medicare and Medicaid programs by the development of health information systems that are private and secure. The Department's proposals promote the safety, efficiency, and effectiveness of the health care system by refining the security standards established by Congress and implemented in the 2003 and 2013 Final Rules. The statute contemplated that the security measures adopted by all regulated entities, including State and local governments, would evolve over time in accordance with the security risks they face, and the NPRM proposals are in the nature of enhancing these existing requirements. Thus, the Department does not believe that the rule would impose substantial direct compliance costs on State and local governments that are not required by statute.

The Department anticipates that the most significant direct costs on State and local governments would be for conducting a Security Rule compliance audit; notifying covered entities or business associates, as applicable, upon activation of a contingency plan; notifying covered entities of changes or termination of workforce members' access to ePHI; deploying MFA; removing extraneous software; and penetration testing; providing or obtaining verification of business associates' compliance with technical safeguards; updating health plan documents; updating policies and procedures; and updating workforce training. However, the costs involved can be attributed to the statutory requirements of the Administrative Simplification provisions of

---

HIPAA. Sec. 264 of HIPAA contains the provisions pertaining to the privacy of individually identifiable health information.

HIPAA and would be similar in kind to those borne by non-government-operated regulated entities, which the proposed RIA above addresses in detail.

In considering the principles in and requirements of E.O. 13132, the Department believes that these proposed modifications to the Security Rule would not significantly affect the rights, roles, and responsibilities of the States and requests comment on this analysis.

E. Assessment of Federal Regulation and Policies on Families

Section 654 of the Treasury and General Government Appropriations Act of 1999[90] requires Federal departments and agencies to determine whether a proposed policy or regulation could affect family well-being. If the determination is affirmative, then the Department or agency must prepare an impact assessment to address criteria specified in the law. This proposed rule is expected to strengthen family well-being because it would ensure a baseline of security measures for individuals' PHI, and medical information and decisions based on that information are at the heart of family decision making. If finalized, the provisions in this proposed rule may be carried out only by the Federal Government because it would modify Federal law on cybersecurity in health care, ensuring that American families have confidence that the privacy of their PHI is secured by consistent safeguards, regardless of the State where they are located when health care is provided. Such health care privacy and is vital for individuals who seek or access health care.

F. Paperwork Reduction Act of 1995

Under the PRA,[1032] agencies are required to submit to OMB for review and approval any reporting or recordkeeping requirements inherent in a proposed or final rule and are required to publish such proposed requirements for public comment. To fairly evaluate whether an information collection should be approved by the OMB, section 3506(c)(2)(A) of the PRA requires that the Department solicit comment on the following issues:

---

[90] Pub. L. 105–277, 112 Stat. 2681-528 (Oct. 21, 1998) (codified at 5 U.S.C. 601 note). [1032] Pub. L. 104–13, 109 Stat. 163 (May 22, 1995) (codified at 44 U.S.C. 101 note).

1. Whether the information collection is necessary and useful to carry out the proper functions of the agency.

2. The accuracy of the agency's estimate of the information collection burden.

3. The quality, utility, and clarity of the information to be collected.

4. Recommendations to minimize the information collection burden on theaffected public, including automated collection techniques.

The PRA requires consideration of the time, effort, and financial resources necessary to meet the information collection requirements referenced in this section. The Department solicits public comments on its assumptions and burden estimates in this NPRM as summarized below.

In this RIA, the Department proposes to revise certain information collection requirements associated with this NPRM and, as such, would revise the information collection last prepared in 2024 and approved under OMB control # 0945-0003.[91] The proposed revisions to the information collection describe all new and adjusted information collection requirements for regulated entities pursuant to the implementing regulation for HIPAA at 45 CFR parts 160 and 164, the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules").

The estimated annual labor burden presented by the regulatory modifications is 77,067,552 burden hours at a first-year cost of $9,314,106,174. These figures, respectively, represent the sum of 37,781,637 new burden hours at a cost of $4,655,324,954 for compliance by regulated entities and 39,285,915 new burden hours at a cost of $4,658,781,219 for compliance by health plan sponsors.

The overall total burden for respondents to comply with the information collection requirements of all of the HIPAA Privacy, Security, and Breach Notification Rules, including new burdens presented by proposed program changes, is estimated to be 925,144,023 burden hours at a cost of $109,085,104,674, plus $163,499,411 in capital costs for a total estimated

[91] "View ICR," *supra* note 940.

annual burden of $109,248,604,085, after the effective date of the final rule. This estimate is based on a total of 1,202,562,864 responses for a total of 2,565,011 respondents. The total burden for the HIPAA Rules, including the changes proposed in this NPRM, would result in a decrease of 28,838,213 burden hours and a cost increase of $1,911,898,144, in comparison to the baseline in the ICR associated with the 2024 Privacy Rule to Support Reproductive Health Care Privacy.[92] This is the result of multiples changes, such as decreasing burden hours for some existing requirements, increasing the estimated number of covered entities, adding new Security Rule requirements, and expanding the pool of respondents for the Security Rule by adding requirements for health plan sponsors.

Details describing the burden analysis for the proposals associated with this RIA are presented below and explained further in the ICR associated with the NPRM.

1. Explanation of Estimated Annualized Burden Hours

Below is a summary of the significant program changes and adjustments proposed since the approved 2024 ICR; because the ICR addresses regulatory burdens associated with the full suite of HIPAA Rules, the changes and adjustments include updated data and estimates for some provisions of the HIPAA Rules that are not affected by this proposed rule. These program changes and adjustments form the bases for the burden estimates presented in the ICR associated with this NPRM.

Adjusted Estimated Annual Burdens of Compliance

(1) Updating the number of covered entities.

(2) Updating hourly wage rates.

(3) Adjusting downward the number of estimated requests for an exception to Federal preemption of State law to the prior baseline of 1 request per year.

[92] *Id*.

(4) Adjusting downward the estimated hourly burden for regulated entities to report security incidents (not breaches) from 20 hours per monthly report to 10 hours per monthly report.

(5) Updating the number of research disclosures.

New Burdens Resulting from Program Changes

In addition to the adjustments above, the Department proposes to add new annual estimated burdens as a result of program changes, as follows:

(1) A burden of 2 hours for each regulated entity to conduct a Security Rule compliance audit.

(2) A burden of 2 hours for each business associate (including each subcontractor) to provide verification of compliance with technical safeguards.

(3) A burden of .5 hours for each covered entity to obtain verification of business associates' compliance with technical safeguards.

(4) A burden of .083 hours for each business associate to obtain verification of subcontractors' compliance with technical safeguards.

(5) A burden of 1 hour for each regulated entity to provide notification to other regulated entities of workforce members' termination of access to ePHI.

(6) A burden of 1.5 hours for each regulated entity to deploy MFA.

(7) A burden of 4.5 hours for each regulated entity to perform network segmentation.

(8) A burden of .5 hours for approximately 76.56 percent of regulated entities to disable unused ports and remove extraneous software.

(9) A burden of 3 hours for each regulated entity to conduct penetration testing.

(10) A burden of .5 hours for each regulated entity to notify covered entities or business associates, as applicable, upon activation of a contingency plan.

(11) A burden of .5 hours for each insurer and third-party administrator to update health plan documents.

(12) A burden of 2 hours for each regulated entity to update the content of its cybersecurity awareness and Security Rule training program.

(13) A burden of 3.5 hours for each regulated entity to update its policies and procedures.

(14) A burden of 1 hour for each regulated entity to update business associate agreements.

(15) A burden of 52.92 hours for each health plan sponsor to modify safeguards for its relevant electronic information systems to meet Security Rule standards.