Journal of Health Care Law and Policy

Volume 19 | Issue 2 Article 4

Why the Insurance Industry Cannot Protect Against Health Care Data Breaches

Kristen Heald

WHY THE INSURANCE INDUSTRY CANNOT PROTECT AGAINST HEALTH CARE DATA BREACHES

KRISTEN HEALD*

I. INTRODUCTION

On February 4, 2015, millions of Anthem health insurance customers were notified that their personal information might have been accessed in a massive data hack on the nation's second-largest health insurer.[1] The hackers might have obtained the names, birthdays, social security numbers, street addresses, and employment information of as many as eighty million customers.[2] A little over a month later, the health insurance company Premera Blue Cross announced a data breach that exposed the medical and financial data of as many as eleven million customers.[3]

In the first half of 2015 alone, the healthcare sector suffered 187 data breaches that compromised the medical records of eighty-four million patients, and accounted for 21.1% of all breaches worldwide.[4] This wave of high-profile cyber attacks on healthcare organizations marks the beginning of data security breaches, as hackers continue to set their sights on the healthcare industry.[5] Health organizations are an ideal target for hackers looking for large amounts of valuable information.[6] On the black market, credit card information can sell for

* J.D., University of Maryland Francis King Carey School of Law, 2017.

1. Fred Barbash & Abby Phillip, *Massive Data Hack of Health Insurer Anthem Potentially Exposes Millions*, WASH. POST (Feb. 5, 2015), http://www.washingtonpost.com/news/morning-mix/wp/2015/02/05/massive-data-hack-of-health-insurer-anthem-exposes-millions/.

2. Chad Terhune, *Anthem Hack Exposes Data on 80 Million; Experts Warn of Identity Theft,* L.A. TIMES (Feb. 5, 2015), http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html.

3. Kate Vinton, *Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical and Financial Data*, FORBES (Mar. 17, 2015), http://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/.

4. Jack McCarthy, *Healthcare Leads All Industries in Data Breaches*, GOV'T HEALTH IT (Sep. 17, 2015), http://www.govhealthit.com/news/healthcare-leads-all-industries-data-breaches.

5. Andrea Peterson, *2015 is Already the Year of the Health-care Hack – And It's Only Going to Get Worse*, WASH. POST (Mar. 20, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/.

6. *Id.*

as little as one to two dollars per account whereas medical data can fetch around fifty dollars per record.[7] Credit cards can be quickly cancelled if stolen, but medical identity theft is extremely hard to fix, difficult to detect, and much more damaging.[8]

Federal legislation like the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") created federal standards for the handling and use of protected health information ("PHI") and provided incentives for the accelerated adoption of electronic health records ("EHRs") for patients to help doctors share patient data.[9] Although these federal compliance programs were meant to improve healthcare security, the rush to adopt EHR systems in accordance with the federal guidelines has not been coupled with adequate security measures, leaving medical data vulnerable to data breaches.[10] There is no federal law that mandates specific security procedures that industries must follow, and health care organizations have been more focused on delivering health care rather than operational security.[11]

Health care data risks and potential data and monetary losses will force entities to reassess their insurance policies and coverage for data breaches. The ambiguity of traditional coverage directed policyholders to look toward cyber security insurance, a newly emerging market tailored specifically to cyber risks.[12] Because cyberattacks can be unpredictable and costs of data breaches can be difficult to surmount, cyber security insurance can be expensive.[13] Data breaches have not only prompted insurers to increase premiums, but to also raise deductibles and limit coverage for some companies.[14]

This Comment proposes a solution to this crisis, specifically that the federal government should establish a transitional reinsurance program to cover the risks taken by cyber insurance companies to encourage insurers to compete in the new market and result in more affordable premiums. In addition to a risk-shifting

7. Rodika Tollefson, *Healthcare Data at Risk: Why Medical Records Are Easy to Hack, Lucrative to Sell,* THIRDCERTAINTY (Jan. 5, 2015), http://thirdcertainty.com/news-analysis/part-1-healthcare-data-risk-medical-records-easy-hack-lucrative-sell/.

8. *Id.*

9. Cindy Gallee, *The Importance of Data Encryption and Security Rules: Breaches of Electronic Protected Health Information Under HIPAA and HITECH*, 26 J. DUPAGE CTY. BAR ASS'N 16, 17 (2014).

10. Jessica Meyers, *Hackers Threaten Health Care Industry's Patient Records,* BOSTON GLOBE (Sept. 6, 2014), https://www.bostonglobe.com/news/nation/2014/09/05/health-care-industry-ill-prepared-for-vicious-cyberthreats/ZdvDGaipJi7VSN0TogezkL/story.html.

11. *Id.*

12. Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. INFO. TECH. & PRIVACY L. 379, 379 (2014).

13. *Id.* at 384.

14. Jeff Goldman, *Cyber Insurance Premiums Surge in Response to High-Profile Data Breaches*, ESECURITY PLANET (Oct. 21, 2015), http://www.esecurityplanet.com/network-security/cyber-insurance-premiums-surge-in-response-to-high-profile-data-breaches.html.

framework, the government should also act as a risk reducer by providing incentives to promote positive behavior that reduces the overall risk posed by data breaches. Part II will explore the financial burden of data breaches on health care organizations. Part III will assess the current state of insurance coverage for data breaches as distinguished between commercial general liability insurance and cyber insurance. Part IV will discuss why the current framework for protection against data breaches is failing. Finally, Part V will propose legislative solutions aimed at solving this problem.

II. FINANCIAL BURDEN OF DATA BREACHES

A. Federal Regulatory Framework

Overtime, federal legislation has adapted to change the scope and probability of health care risks and the potential liability faced by HIPAA compliant entities.[15] Enforcement for HIPAA breach violations may result in massive penalty payments and drastic increases to the expenses born by the violating organizations.[16]

On August 21, 1996, Congress passed the HIPAA to instigate widespread reform within the health care industry.[17] Two significant goals of HIPAA aimed at curbing the costs of the health insurance industry by reducing health care fraud and creating administrative simplification provisions to encourage the electronic transmission of health information.[18] Recognizing the need to protect patients' medical data in light of electronic advances in health information, Congress included provisions within HIPAA that required the Department of Health and Human Services ("HHS") to adopt national standards concerning the privacy and security of protected health information PHI.[19] In 2000, HHS published a Privacy Rule that set national standards for the protection of the confidentiality of health information and focused on the individual's right to control the use of his or her information.[20] The rule applied to three types of entities: health plans, health care clearinghouses, and most health care providers.[21] In 2003, HHS also published a

15. Arden B. Levy et al., *Data Breaches in Health Care: New or Heightened Risks, Emerging Insurance and Legal Considerations*, ABA SECT. OF LITIG. 2–4 (2014), https://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2014_inscle_materials/written_materials/b10_1_data_breaches_in_health_care.authcheckdam.pdf,

16. *Id.* at 7.

17. Deborah Buckman, *Validity, Construction, and Application of Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Regulations Promulgated Thereunder*, 194 A.L.R. FED. 133 (2004).

18. *Id.*

19. U.S. DEP'T OF HEALTH & HUMAN SERVICES, HIPAA FOR PROFESSIONALS, http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html (last visited Nov.29, 2017).

20. *Id.*

21. *Id.*

Security Rule that required the use of appropriate administrative and technical safeguards to ensure the security of electronic PHI.[22] The Department of Health and Human Services Office of Civil Rights ("OCR") enforces HIPAA through a complaint and investigation process, statutorily mandated audits, fines, and penalties.[23]

The Health Information Technology for Economic and Clinical Health Act ("HITECH") was passed as a part of the American Recovery and Reinvestment Act of 2009 ("ARRA").[24] HITECH strengthened HIPAA Privacy and Security Rules by adding a breach notification requirement and enhancing penalties for violations.[25] The HITECH Act also "granted State attorney generals the authority to enforce HIPAA rules by bringing civil actions on behalf of state residents in federal district court."[26]

Important modifications to both HITECH and HIPAA were made with the effectuation of HHS's Omnibus Rule on March 26, 2013.[27] The Omnibus Rule made a number of changes that broadened liability of health organizations, increased penalties for violations, and changed the standards for what constitutes a breach.[28] The new rule changed the scope of liability to make not only health care providers directly liable to HIPAA Privacy and Security requirements, but to make their business associates directly liable, as well.[29] Business associates are defined in the Omnibus Rule as a "person who 'creates, receives, maintains, or transmits' protected health information on behalf of a covered entity."[30] The rule introduced circumstances under which covered entities may be liable for a HIPAA violation based on the conduct of their business associates.[31] The federal common law of agency is used to determine culpability and turns on the right or

22. *Id.*

23. U.S. DEP'T OF HEALTH & HUMAN SERVICES, HOW OCR ENFORCES THE HIPAA PRIVACY & SECURITY RULES, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html (last visited Nov. 29, 2017).

24. *See* Gallee, *supra* note 9, at 16.

25. *Id.* at 17.

26. HIPAA FINAL RULE: ENFORCEMENT BY STATE ATTORNEYS GENERAL, http://www.hipaa.com/hipaa-final-rule-enforcement-by-state-attorneys-general/ (last visited Nov. 29, 2017) [hereinafter HIPAA FINALRULE].

27. Jerold Oshinsky et al., *Does Your Insurance Policy Protect Against Liability Under the New HIPAA Regulations?*, URMIA J. 69, 69 (2013), https://higherlogicdownload.s3.amazonaws.com/URMIA/afec0d8f-84a3-4a20-a673-b744a68477fd/UploadedFiles/URMIAJournal2013_WEB.pdf.

28. *Id.*

29. *Id.* at 70.

30. Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5572 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

31. 78 Fed. Reg. 5566, 5581 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

authority of the health provider to control the business associate's conduct in the course of performing a service on its behalf.[32]

Another important aspect of the 2013 Omnibus Rule was its amendment to the Breach Notification Rule for Unsecured Protected Health Information set under HITECH.[33] HITECH defined a *breach* as the "unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information."[34] The rule required a finding that "compromise[ed]" data posed a "significant risk of financial, reputational, or other harm to the individual."[35] If this harm standard was met, health care providers were required to notify patients of the breach.[36]

The Omnibus Rule eliminated the "significant risk of harm" standard and moved toward a more stringent presumption of harm standard.[37] The new regulations presume a breach whenever PHI is acquired, accessed, used or disclosed in a way that violates the Privacy Rule.[38] The breach must be reported unless the covered entity demonstrates that there is a "low probability the protected health information has been compromised."[39] The risk assessment focuses on four factors: 1) the nature and extent of the PHI involved; 2) the unauthorized person who used the PHI or to whom the disclosure was made; 3) whether the PHI was actually acquired or viewed; and 4) the extent to which the risk to PHI has been mitigated.[40] In bringing about this change, HHS explained, in the preface to the Omnibus Rule, that the previous harm standard was too subjective and set too high a bar for triggering breach notification.[41]

The Omnibus Rule significantly increased the risk and scope of culpability on the part of health care providers for breach notification and for the actions of their business associates. In addition to this heavy burden, the rule also increased the amount of civil penalties for HIPAA violations, which start at $100 per violation and increase up to $50,000 per violation, with a yearly maximum of $1.5 million, depending on the nature of the violation.[42] There are four categories of violations reflecting increasing levels of culpability and the corresponding penalty amounts for each.[43] The baseline for a violation is establishing the covered entity did not know or have reason to know of the violation, despite exercising

32. *Id.*
33. *Id.*
34. *Id.* at 5369.
35. *Id.*
36. *Id.* at 5638.
37. Oshinsky, *supra* note 27, at 69–70.
38. *Id.*
39. See s*upra* note 30, at 5641.
40. 78 Fed. Reg. 5566, 5642 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).
41. *Id.* at 5641.
42. 42 U.S.C. § 1320d-5(a) (2013).
43. 78 Fed. Reg. 5566, 5583 (Jan. 25, 2013) (codified at 45 C.F.R. pts. 160, 164).

reasonable diligence.[44] The highest culpability for a violation is established when it is shown the violation was due to willful neglect and not timely corrected.[45]

B. Cost Breakdown

Calculating the cost of a data breach is not a straightforward process. The financial repercussions are just coming to light in the industry, and it might take years to assess the full impact of any given incident.[46] Financial penalties are being issued with increasing frequency to health care organizations for HIPAA violations and reports of breaches continue to rise.[47] The value of PHI on the black market and the inability of customers to change information, like social security numbers and street addresses once stolen, makes curing a breach that much harder to resolve.[48] Researchers have calculated the average cost of a breach in 2015 at $363 per medical record.[49] Breaches in health care are the most expensive to remediate and are only growing more costly.[50] In the U.S. healthcare industry, the average cost of a breach is $398 per medical record.[51] This sum is far higher than the average cost of a data breach across most other industries at $154 per record.[52] Moreover, data breaches cost the healthcare system an estimated $6 billion annually.[53] Many costs are hard to predict and are dependent on the size of the breach; however, it is extremely important to calculate potential loss in order to assess the type of coverage needed.[54]

According to the *HIPAA Journal*, there are a variety of different sources of costs that organizations should be aware of when calculating the financial impact of a data breach.[55] First is the cost of a breach investigations, in which an external organization must investigate to identify the the cause and source of the breach.[56]

44. *Id.* at 5582–83.

45. *Id.* at 5583.

46. *Calculating the Cost of a HIPAA Data Breach,* HIPAA J. (Apr. 30, 2015), http://www.hipaajournal.com/calculating-the-cost-of-a-hipaa-data-breach-6534/ (last visited Nov. 29, 2017) [hereinafter *Calculating the Cost*].

47. *Id.*

48. Tod Ferran, *The Cost of HIPAA Breach Insurance*, SECURITY METRICS BLOG (June 15, 2015), http://blog.securitymetrics.com/2015/06/the-cost-of-hipaa-breach-insurance.html (last visited Nov. 29, 2017).

49. Joseph Conn, *Healthcare Data Breaches Are Costliest: Study*, MODERN HEALTHCARE (May 28, 2015), http://www.modernhealthcare.com/article/20150528/NEWS/150529899.

50. *Id.*

51. *Id.*

52. *Id.*

53. PONEMON INST., CRIMINAL ATTACKS ARE NOW LEADING CAUSE OF DATA BREACH IN HEALTHCARE, ACCORDING TO NEW PONEMON STUDY (May 7, 2015), https://www.ponemon.org/news-2/66.

54. Ferran, *supra* note 48 (advising that cyber security insurance is important for healthcare providers as the devastating effects of a breach can result in an unspecified amount of financial damage).

55. *Calculating the Cost*, *supra* note 46.

56. *Id.*

In the case of a breach, the OCR oversees the organization's spending of remediation costs, which go into implementing the safeguards that should have been in place initially to prevent the breach.[57] Temporary operational changes after a breach require spending on issuing notifications, answering customer questions, updating social media sites, and implementing new safeguards.[58] Breach notification requirements mandate that letters must be issued to all affected individuals by first class mail at a current cost of forty-nine cents per letter.[59] The *HIPAA Journal* estimates that one letter issued to all individuals affected by the breach could cost Anthem $40 million in postage costs alone.[60]

The HHS included in the Omnibus Rule a summary of annual breach notification compliance costs in 2011 indicating it totaled $14,475,600.[61] These costs include: E-mail and first class mail ($3,467,122); Substitute Notices: Media Notice ($571,200); Substitute Notices: Toll-Free Number ($1,816,379); Imputed Cost to Affected Individuals Who Call the Toll-Free Line ($2,042,665); Notice to Media of Breach: Over 500 People ($15,420); Report to HHS: 500 or More ($15,420); Investigation Costs: Under 500 ($5,277,456); Investigation Costs: 500 or More ($837,500); and Annual Report to the Secretary ($422,438).[62] Consequently, the larger the number of individuals affected from a breach, the higher these breach notification costs will be.

HIPAA requires that entities provide free identity theft and credit monitoring services to all individuals affected for one to two years after the breach.[63] This is estimated to cost $10 per individual, per month.[64] As previously discussed, regulatory fines issued by the OCR are another source of expenses that can cost as much as $1.5 million per year, per violation.[65] According to the HHS website, the highest fine ever issued was in 2014 to New York Presbyterian Hospital/Columbia University Medical Center for $4.8 million in violations.[66] The electronic PHI of 6,800 patients was impermissibly disclosed to Google.[67] An alternate source of regulatory fines can come from Attorney Generals, who have the authority to assist the OCR in enforcing HIPAA Privacy and Security Rules.[68]

57. *Id.*

58. *Id.*

59. *Id.*

60. *Id.*

61. See s*upra* note 30, at 5671.

62. *Id.* at 5670–75.

63. *Calculating the Cost*, *supra* note 46.

64. *Id.*

65. *Id.*

66. U.S. DEP'T OF HEALTH & HUMAN SERVICES, DATA BREACH RESULTS IN $4.8 MILLION HIPAA SETTLEMENTS (May 7, 2014), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html (last visited Nov. 29, 2017).

67. Lauren Friedman, *Hospital to Pay Millions After Embarrassing Data Breach Put Patient Info on Google*, BUS. INSIDER (May 9, 2014).

68. HIPAA FINAL RULE, *supra* note 26.

HITECH authorizes State Attorney Generals to impose fines up to $25,000 per violation category, per year.[69] Another cost that may often be unforeseeable to an organization is the loss of business or reputation.[70] A Ponemon study found that the healthcare industry has one of the highest customer churn rates (measure of patients who discontinue service) at six percent, which suggests that the healthcare industry could reduce data breach costs by putting more emphasis on customer retention.[71]

Finally, class-action lawsuits can be a huge source of loss for providers in the wake of a breach.[72] Three lawsuits were filed against Anthem less then twenty-four hours after the breach announcement.[73] Shortly after, a woman claiming $5,000,000 in damages filed a class action suit against Anthem.[74] Health care data breach lawsuits typically claim damages of $1,000 per victim.[75] However, as in Anthem's case, these estimates could greatly exceed that amount in cases where a large number of patients have been harmed. These exorbitant costs will only continue to rise in the wake of enhanced federal enforcement, increased fines and penalties, broader liability, and larger scale data breaches that affect millions of patients. It is increasingly important for health care entities to have appropriate insurance coverage to help mitigate the potentially devastating impact of a data breach.

Data breaches are unquestionably expensive and one would think that the cost alone would incentivize companies to improve practices and safeguard patient data. The Anthem data breach is estimated to cost well over $100 million.[76] To any small business, those costs would be devastating. However, to the multi-billion dollar company, the cost of $100 million (much of which would be offset by insurance) is a mere .01% of its annual revenue.[77] To large corporations like Anthem, the cost and effort to improve security defenses is simply not worth it.[78] This point is important to factor in when considering remedies that not only take on economic risk but also incentivize companies to invest in security solutions across the board.

69. *Id.*

70. *Calculating the Cost*, *supra* note 46.

71. PONEMON INST., 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 16 (2015).

72. *Calculating the Cost*, *supra* note 46.

73. Mary A. Chaput, *Calculating the Colossal Cost of a Data Breach*, CFO (Mar. 24, 2015), http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/.

74. Mike Gauntner, *Warren Woman Files $5,000,000 Suit over Anthem Data Breach*, WFMJ (Apr. 5, 2015), http://www.wfmj.com/story/28725895/warren-woman-files-5000000-suit-over-anthem-data-breach.

75. Chaput, *supra* note 73.

76. Taylor Armerding, *Breach Costs: 'Chump Change' to Bottom Lines of Big Players*, CSO (June 8, 2015), http://www.csoonline.com/article/2932324/data-breach/breach-costs-chump-change-to-bottom-lines-of-big-players.html.

77. *Id.*

78. *Id.*

III. INSURANCE COVERAGE FOR DATA BREACHES

A. Traditional Insurance Coverage

Insurance manages risk and provides financial compensation in the event of a loss. Understanding the financial impact of a data breach allows an organization to choose coverage that will most effectively mitigate these losses and risks. A Commercial General Liability ("CGL") policy is the traditional insurance policy issued to business organizations to protect against liability for claims of bodily injury, property damage, and advertising and personal injury liability.[79] This is the most common type of insurance policy and is the first place policyholders look when determining coverage.[80] Data breach coverage disputes focus on Coverage A: Bodily Injury and Property Damage Liability and Coverage B: Personal and Advertising Injury Liability offered under a CGL policy.[81] The debate stems from whether there is "property damage" or "personal injury" in data breach cases.[82]

The term "property damage" under Coverage A most often requires physical damage to "tangible property" and specifically excludes coverage for software, data, or information stored in an electronic format.[83] More often than not, courts will decline to extend coverage of "tangible property" to electronic data, unless there is physical damage or loss of use of a tangible product, like a computer.[84]

Under Coverage B, "personal injury" is defined to include "oral or written publication, in any manner, of material that violates a person's right of privacy."[85] CGL coverage for data breaches under "personal injury" largely centers on if there has been a "publication" of the compromised information that would warrant coverage.[86] Courts have struggled with the definition of "publication" over the years and have made contradictory rulings about whether CGL policies

79. *Commercial General Liability (CGL) Policy,* IRMI, http://www.irmi.com/online/insurance-glossary/terms/c/commercial-general-liability-cgl-policy.aspx.

80. Gregory D. Podolak, *Insurance for Cyber Risks: A Comprehensive Analysis of the Evolving Exposure, Today's Litigation, and Tomorrow's Challenges,* 33 QUINNIPIAC L. REV. 369, 382 (2015).

81. Alex E. Pontente et al., DRI's Data Breach and Privacy Law Seminar, Insurance Coverage Issues Implicated in Data Breach Claims, SEDGWICK LLP 403, 406 (Sept. 12, 2014).

82. *Id.*

83. *Id.*

84. *Id.*; *see* Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (8th Cir. 2010) (finding property damage to a computer when it froze and became inoperable); *see also* American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc., No. 99-185 TUC ACM, 2000 WL 726789, *4 (D. Ariz. Apr. 18, 2000) (holding a computer system did not suffer "physical damage" as a result of a power outage).

85. Pontente et al., *supra* note 81, at 406–07.

86. Podolak, *supra* note 80, at 383.

extend coverage to data breaches on this basis.[87] *Zurich American Insurance v. Sony Corp. of America*[88] was a 2014 data breach case in which the Court found that there was no coverage available to Sony under its CGL policy.[89] The hack stole the personal information of tens of millions of Sony PlayStation users and Sony sought coverage under the "personal injury" component of its CGL policy, arguing that the breach constituted a "publication" of private information.[90] The Court found that a CGL policy requires the policyholder to actually commit the act, and since hackers, and not Sony, perpetrated the "publication" of information here, it therefore did not qualify for coverage.[91] Since *Zurich*, the general consensus seems to be that CGL policies provide little to no coverage for liabilities resulting from data breaches.[92]

Recognizing the confusion in courts over CGL coverage and the increasing risks of data breaches, Insurance Services Office Inc. ("ISO"), which develops standard insurance contract language, released an exclusion expressly limiting Coverage A and B to exclude coverage "for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information."[93] Moreover, "the exclusion will apply even if damages are claimed for notification costs, credit monitor expenses . . . or any other loss . . . incurred . . . with respect to that which is subject to the exclusion."[94] Provisions such as these, as well as the general inapplicability of traditional CGL coverage to data breaches, has demonstrated a need to transfer risk from traditional lines to a more specific product tailored to cyber policies.

87. Jana Landon, *Where Does Sony Settlement Leave CGL Insurance for Data Breaches?,* LEGAL INTELLIGENCER (May 13, 2015), https://www.law.com/thelegalintelligencer/almID/1202726345560/?slreturn=20171029121429; *see* Butts v. Royal Vendors, 202 W.Va. 448 (1998) (holding there is no coverage for "publication of material" that violates a third party's right to privacy); *see also* Recall Total Info Mgmt. v. Federal Ins., 83 A.2d 667 (Conn. App. Ct. 2014) (holding theft of information alone is insufficient to find a "publication" under a CGL policy); Hartford Cas. Ins. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx) (Oct. 7, 2013) (holding the CGL policy covered a hospital data breach despite insurance policy exclusion for personal and advertising injury).

88. Zurich American Ins. v. Sony Corp. of America, No. 651982/2011, 2014 WL 3253541 (N.Y. Sup. Ct. Feb. 21, 2014) (No. 525).

89. *Id.*

90. Landon, *supra* note 87.

91. *Id.*

92. Jes Alexander, *Anatomy of a Data Breach: What Cyber Policies Should Cover,* 13 J. TEX. INS. L. 5 (2015).

93. Tatiana Melnik, *Cyberliability Insurance: To Buy or Not to Buy?,* 17 J. HEALTH CARE COMPLIANCE 51, 52–53 (2015).

94. *Id.* at 53.

B. Cyber Insurance

As insurers and courts are increasingly reluctant to extend CGL coverage to data breaches, it should come as no surprise that standalone cyber security policies are on the rise.[95] As more high-profile cyber attacks happen, health organizations are increasing their investment in cyber insurance to help mitigate their risk exposure in the case of a breach.[96] Healthcare entities increased their cyber spending to forty-one percent in 2015.[97] An estimated $2 billion worth of health-related cyber insurance was sold in 2014, and the market is growing at twenty to twenty-five percent per year.[98]

A robust cybersecurity insurance market would help reduce cyber attacks by promoting the adoption of better security practices in exchange for more coverage and lower rates.[99] Policyholders could devote more resources to their cybersecurity infrastructure and actively work to improve the quality of data collection and monitor cyber threats.[100] Insurers could offer reduced premiums to those seeking coverage if they take steps to decrease the extent of the insurer's liability, which would increase competition and lower market prices.[101] This could shift the focus of health care organizations to the value of security implemented, rather than simply complying with baseline protocols. A healthy, competitive cyber insurance market could provide a fluid system to minimize damage and recovery time in the aftermath of a data breach.

However, despite increasing demand for cyber insurance, this ideal model of a competitive, affordable market has yet to be achieved. A standardized assessment of cyber risk does not yet exist.[102] The relatively new market for cyber insurance creates a difficult risk to price by traditional insurance methods since there is a lack of actuarial data available.[103] The unpredictable probability and nature of data breaches, paired with the unknown impact of long-term financial

95. Garrie & Mann, *supra* note 12, at 384.

96. Patricia Harman, *Cyber Attacks Drive Insurance Purchases in Early 2015*, PROPERTYCASUALTY360 (Oct. 22, 2015), http://www.propertycasualty360.com/2015/10/22/cyber-attacks-drive-insurance-purchases-in-early-2.

97. *Id.*

98. Arthur Allen, *Billions to Install, Now Billions to Protect,* POLITICO (June 6, 2015), http://www.politico.com/story/2015/06/health-care-spending-billions-to-protect-the-records-it-spent-billions-to-install-118432.

99. Laura A. Odell, *Cyber Insurance – Managing Cyber Risk,* INST. FOR DEF. ANALYSIS 1, 4 (Apr. 2015).

100. *Id.*

101. Liam M.D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance*, 3 J.L. CYBER WARFARE 1, 18–19 (2014).

102. *Id.* at 8–9 (stating a comprehensive cyber security system is difficult to create as each industry that requires cyber security development has a markets with different needs).

103. Leigh Thomas & Jim Finkle, *Insurers Struggle to Get Grip on Burgeoning Cyber Risk Market*, REUTERS (July 14, 2014), http://www.reuters.com/article/2014/07/14/us-insurance-cybersecurity-idUSKBN0FJ0B820140714?feedType=RSS&feedName=businessNews.

loss, makes it extremely hard for insurers to adequately assess actual risks for a given company and leaves them unprepared for a catastrophic cyber event.[104] Typically, insurance companies purchase reinsurance from other insurance companies to spread risk and limit the total loss the original insurer would experience in the event of a disaster.[105]

The rise of data breaches has prompted insurers to significantly increase cyber premiums and deductibles while capping coverage at $100 million.[106] Some estimates conclude that a company may need as much as $1 billion in cyber insurance to protect its assets, but most companies will be unable to secure more than $300 million.[107] Health insurance companies that have experienced a data breach seem to be hit the hardest, with some premiums tripling on renewal.[108] Anthem ran into difficulties renewing its coverage in the aftermath of the data breach, managing to get $100 million in coverage, but only with a $25 million deductible.[109] High-profile data hacks are finally giving insurers a little insight into the financial impact of a breach, and the results are devastating.[110] The high cost of cyber security insurance may put health care companies in the position of choosing between spending money on cyber insurance or investing those funds into better cyber security infrastructure.[111]

IV. THE CURRENT FRAMEWORK IS FAILING

The rise of data breaches exposed the failure of existing safeguards and mechanisms to not only protect against these risks, but to prevent them from reoccurring in the future. Cyber insurance coverage will not, in itself, fully mitigate the risk posed by data breaches. As previously mentioned, for large companies like Anthem, the cost of a data breach amounted to a mere .01% of its annual revenue.[112] Most corporations in this position would rather write off the losses than spend two to three times that on heightened security measures.[113] From a

104. Odell, *supra* note 99, at 3.

105. Steven Merkel, *What Is Reinsurance?,* INVESTOPEDIA http://www.investopedia.com/ask/answers/08/reinsurance.asp.

106. Goldman, *supra* note 14.

107. Clinton Karr, *Shifting Cyber Insurance Rates Creates New Dilemmas*, BROMIUM BLOG (Oct. 30, 2015), http://blogs.bromium.com/2015/10/30/shifting-cyber-insurance-rates-creates-new-dilemmas/ (last visited Nov. 29, 2017).

108. Goldman, *supra* note 14.

109. *Id.*

110. *See id.* (noting the cyber security attacks resulted in enormous costs to healthcare companies and their clients).

111. *Id.* (finding as a result of the financially devastating cyber security attacks, many healthcare companies are re-evaluating how to maximize their company's security through cyber insurance).

112. Armerding, *supra* note 76.

113. *Id.*

purely financial perspective, the possibility of a massive data breach is quite rare, so improving data security practices seems like a waste of money.[114]

There is little to no incentive for health care organizations to invest in digital security as a proactive approach to preventing data breaches.[115] Cyber insurance coverage is a reactive protection measure that bears part of the risk, but does nothing to motivate health entities to reduce the risk firsthand.[116] This is a classic moral hazard problem, meaning that when financially protected through insurance, an individual's motives and behavior to prevent loss are reduced, resulting in an increased probability of loss.[117] Risk transfer can either lead to more risky behaviors, or incentivize positive behaviors through the implementation of prevention measures.[118] Thus, any realistic remedy to the data breach problem must reallocate economic risk to kick-start the cyber insurance market and incentivize cyber insurers to effectuate security measures to reduce overall risk.

V. LEGISLATIVE SOLUTIONS

A. Federal Government Reinsurance Program

The federal government as reinsurer could help stimulate and prioritize the cyber insurance market. The infancy of the market for cyber insurance impedes its growth as an industry due to a scarcity of data and a high level of uncertainty that causes insurers to raise premiums and lower coverage.[119] Coverage limits should encompass a majority of a policyholder's loss; however, uncertainty as to the full extent of loss means there are many indirect effects from cyber losses that cannot be measured and thus not covered.[120]

A transitional federal reinsurance program could subsidize insurance costs and help the market remain afloat until cyber reinsurers can get a better sense of data and risk for more affordable premiums.[121] This could increase the supply of

114. *Id.*

115. Niam Yaraghi & Joshua Bleiberg, *The Anthem Hack Shows There Is No Such Thing as Privacy in the Health Care Industry*, BROOKINGS (Feb. 12, 2015), http://www.brookings.edu/blogs/techtank/posts/2015/02/12-anthem-hack-health-privacy.

116. *Id.*

117. Swenja Surminski, *The Role of Insurance in Reducing Direct Risk–The Case of Flood Insurance,* INT'L REV. OF ENVTL. & RESOURCE ECON. 241, 242–43 (2013).

118. *Id.* at 243.

119. Christian Biener et al., *Insurability of Cyber Risk: An Empirical Analysis*, U. ST. GALLEN, (Jan. 2015), https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf.

120. *Id.* at 18.

121. Larry Clinton, *Cyber-Insurance Metrics and Impact on Cyber-Security*, INTERNET SECURITY ALLIANCE WHITE PAPER (undated), https://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf.

cyber insurance, reduce prices, and increase competition in the market.[122] Guaranteed reinsurance for a breach from the federal government could make insurers feel more secure in offering large amounts of cyber insurance coverage to those companies that need it.[123] Ultimately, insurance companies need to know more about the likelihood of a breach, how breaches should be valued, and how to measure the effectiveness of cybersecurity risk management strategies designed to address them.[124] A reinsurance program could promote the security insurance companies' need to join and compete in the market and create time in which relevant actuarial data can be developed until enough information exists for the market to be able to fully stand on its own.[125]

The federal government acting as a reinsurer of last resort in the event of catastrophic loss is not a new concept.[126] The Terrorism Risk Insurance Act of 2002 ("TRIA"), administered by the U.S. Department of Treasury, created a temporary federal reinsurance program that, in the event of a major terrorist attack, allows the insurance industry and federal government to share losses.[127] TRIA offers a measure of certainty to the insurance industry as to the maximum size of losses insurers would have to pay and is triggered when losses exceed a certain amount.[128] The law has had positive effects on the insurance market, with roughly sixty percent of commercial policyholders purchasing coverage over the past few years and generally pushing prices for terrorism insurance downward.[129]

However, it is important to note that TRIA was meant to be a "temporary" subsidy program while the financial services industry developed the "systems, mechanisms, products, and programs necessary to create a viable . . . market for private terrorism risk insurance."[130] The Act was originally set to expire in 2005,

122. *Id.*

123. *Id.*

124. U.S. DEP'T OF HOMELAND SECURITY, CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT 1, 4 (Nov. 2012), https://www.dhs.gov/sites/default/files/publications/November%202012%20Cybersecurity%20Insurance%20Workshop.pdf 12), (finding that awareness for potential cyber security breaches has led to companies investigating pro-active methods to combat these concerns).

125. *Id.* at 35.

126. M. Martin Boyer & Charles M. Nyce, *An Industrial Organization Theory of Risk-Sharing*, 17 NORTH AM. ACTUARIAL J. 283, 283 (Nov. 26, 2013).

127. Caroline McDonald, *TRIA Signed into Law by President Obama – Terrorism Risk Insurance Act,* NAT'L L. REV. (Jan. 18, 2015), http://www.natlawreview.com/article/tria-signed-law-president-obama-terrorism-risk-insurance-act.

128. INS. INFO. INST., TERRORISM & RISK INSURANCE (Jun. 2015), http://www.iii.org/issue-update/terrorism-risk-and-insurance.

129. Baird Webel, *Terrorism Risk Insurance: Issue Analysis and Overview of Current Program*, CONG. RES. SERV. (Jul. 23, 2014).

130. Diane Katz, *TRIA: Time to End Years of "Temporary" Insurance Subsidies*, DAILY SIGNAL (July 16, 2014), http://dailysignal.com/2014/07/16/tria-time-end-years-temporary-insurance-subsidies/.

but has been renewed three times since, most recently in January 2015 for another six years after Congress allowed it to expire on December 31, 2014.[131] Critics of the Act point out the program's shifting of the potential costs of terrorist losses from businesses to taxpayers.[132] Others argue that continued federal involvement in terrorism insurance is hindering the private insurance market from developing capabilities to be able to handle this risk on its own.[133] The Department of Treasury cautioned the public about renewing the program, "noting that it was meant to be temporary, and urging more reliance on the private sector."[134]

The National Flood Insurance Program ("NFIP"), while not a federal reinsurance program, provides an example of federal government intervention aimed at filling a gap in the insurance market.[135] In 1968, Congress created the NFIP to help provide flood insurance to property owners.[136] The catastrophic effects of floods were causing enormous losses to life and property, and the only financial recourse available to victims was in disaster assistance.[137] Private insurance companies could not provide flood insurance coverage at an affordable price due its devastating nature and the lack of an actuarial rate structure to reflect the risk.[138]

The NFIP, administered by the Federal Emergency Management Agency ("FEMA"), is a voluntary program through which participating communities agree to adopt and enforce regulation of floodplain development to reduce future flood damages.[139] In return, property owners within a participating community may elect to purchase federally backed flood insurance.[140] FEMA works closely with more than eighty private insurance companies to offer flood insurance to these communities at nationally established (below-market) rates.[141] The revenue

131. U.S. DEP'T OF THE TREASURY, TERRORISM RISK INSURANCE PROGRAM, https://www.treasury.gov/resource-center/fin-mkts/Pages/program.aspx.

132. INS. J., *Debate over Terrorism Insurance to be Renewed* (Feb. 6, 2013), http://www.insurancejournal.com/news/national/2013/02/06/280332.htm.

133. *Id.*

134. *Id.*

135. NAT'L FLOOD INS. PROGRAM, ABOUT THE NAT'L FLOOD INSURANCE PROGRAM: OVERVIEW, https://www.floodsmart.gov/floodsmart/pages/about/nfip_overview.jsp (last visited Nov. 29, 2017).

136. *Id.*

137. FED. EMERGENCY MGMT. AGENCY, NAT'L FLOOD INSURANCE PROGRAM: PROGRAM DESCRIPTION (Aug. 1, 2002), http://www.fema.gov/media-library-data/20130726-1447-20490-2156/nfipdescrip_1_.pdf (last visited Nov. 29, 2017).

138. *Id* at 1.

139. *Id.* at 12.

140. *Id.* at 2.

141. NAT'L FLOOD INS. PROGRAM, THE NFIP PARTNERSHIP, https://www.floodsmart.gov/floodsmart/pages/about/nfip_partnership.jsp (last visited Nov. 29, 2017).

collected from the purchased policies help to pay for claims, but when claims exceed revenues, the NFIP is authorized to borrow from the U.S. Treasury.[142]

While the NFIP has undoubtedly reduced claims from flood risk and future damages by increasing preparedness standards and flood insurance adoption, financial concerns led the U.S. General Accounting Office to determine that the program is not actuarially sound.[143] This suggests that premiums collected for policies are insufficient to serve as a reserve for paying out potential catastrophic losses.[144] The subsidized premiums offered under the NFIP do not actually reflect the risk associated with properties, and they resulted in net annual losses as high as $600 million.[145] NFIP borrowed billions of dollars from the Treasury Department to cover claims from devastating natural disasters, like Hurricane Katrina, and by 2014, the continued borrowing caused the program to incur a total of $23 billion in debt.[146] One of the possible solutions proposed to remedy this debt is to keep the federal government as the primary line of flood insurance, but to pay a reinsurance premium to the private sector to take on losses exceeding a loss amount or based on particular flood disaster size.[147]

The final and most recent precedent for federal government reinsurance can be found in the 2010 Affordable Care Act ("ACA").[148] The ACA is a comprehensive health reform law aimed at providing more affordable healthcare, expanding coverage, and improving the health care delivery system.[149] The law requires most U.S. citizens to enroll in health insurance plans and requires states to establish health insurance exchanges, through which private insurers sell plans, in compliance with ACA regulations.[150] Enrollees whose household income falls between 100% and 400% of the federal poverty level can receive federal premium subsidies on plans purchased through these state exchanges.[151]

142. NAT'L ACAD. OF SCI., AFFORDABILITY OF NAT'L INSURANCE PROGRAM PREMIUMS (Mar. 2015), http://dels.nas.edu/resources/static-assets/materials-based-on-reports/reports-in-brief/Affordability-of-NFIP-final.pdf (last visited Nov. 29, 2017).

143. U.S. GOV'T ACCOUNTABILITY OFFICE, HIGH RISK SERIES: AN UPDATE (Feb. 2015), http://www.gao.gov/assets/670/668415.pdf (last visited Nov. 29, 2017).

144. *Id.*

145. Loren M. Vasquez, *Big Storms, Big Debt, and Biggert-Waters: Navigating Florida's Uncertain Flood Insurance Future,* SEATTLE J. ENVTL. L. 110, 118–19 (May 31, 2015).

146. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 143.

147. Mark A. Hofmann, *Rollback of NFIP Reforms Has Reinsurers Re-evaluating Private Market,* BUS. INS. (May 11, 2014), http://www.businessinsurance.com/article/20140511/NEWS04/305119979.

148. Angela Boothe & Brittany La Couture, *The ACA's Risk Spreading Mechanisms: A Primer on Reinsurance, Risk Corridors and Risk Adjustment*, AM. ACTION FORUM (Jan. 9, 2015).

149. THE HENRY J. KAISER FAMILY FOUNDATION, SUMMARY OF THE AFFORDABLE CARE ACT (Apr. 25, 2013), http://kff.org/health-reform/fact-sheet/summary-of-the-affordable-care-act/.

150. Boothe & La Couture, *supra* note 148.

151. *Id.*

The ACA brought a big change to how insurers offered plans in that it prohibits insurers from denying coverage to people, excluding pre-existing conditions or varying premiums based on health status.[152] Not knowing how many people will enroll, or the proportion of sick beneficiaries, creates more uncertainty and larger risk for insurance providers in this new market.[153] To improve incentives for insurers to participate and limit the amount an insurance company can lose in the marketplace, the ACA created three risk-sharing programs: a permanent risk adjustment program, a temporary risk-corridor program, and a transitional reinsurance program.[154]

The permanent risk adjustment program aims to reduce incentives for health insurance plans to enroll people with higher than average costs. This is achieved by having plans with lower than average actuarial risk make payments to those plans whose individuals have higher than average risk.[155] The HHS or state exchanges assess the actuarial risk of the insurance pool within each plan and compare it to the average of all the plans in the state in order to shift the money accordingly.[156]

The temporary risk corridors program mitigates pricing uncertainty (of who will enroll and what their health spending will be) by sharing gains and losses between plans and the federal government.[157] Actual claims are compared to expected claims assumed in the insurer's premiums.[158] If actual claims exceed or fall below expected claims by more or less than three percent, HHS will either reimburse the plan for at least fifty percent of excess loss, or the plan will pay HHS at least fifty percent of the excess gained.[159]

The risk corridor program was not originally required to be budget neutral; however, the 2015 Cromnibus Bill mandated that "2014 risk corridors receivables paid in 2015 be funded through payables into the program from other insurers."[160] This legislation came after 2014 insurance premiums had already been set and when most insurers "anticipated receiving full payment for the money the government owed under the risk corridors program."[161] The result is a "$2.5 billion shortfall between the money taken in under the program and the money

152. AM. ACAD. OF ACTUARIES, FACT SHEET: ACA RISK-SHARING MECHANISMS 1 (2013).

153. *Id.*

154. *Id.*

155. *Id.*

156. Boothe & La Couture, *supra* note 148.

157. AM. ACAD. OF ACTUARIES, *supra* note 152, at 2.

158. *Id.*

159. *Id.*

160. Scott Katterman, *Headwinds Cause 2014 Risk Corridor Funding Shortfall*, MILLIMAN (Oct. 5, 2015), http://us.milliman.com/insight/2015/Headwinds-cause-2014-risk-corridor-funding-shortfall/.

161. Seth Chandler, *Bad News for ObamaCare: Insurers Lost a Lot of Money in 2014*, ACA DEATH SPIRAL (Oct. 2, 2015), http://acadeathspiral.org/2015/10/02/bad-news-for-obamacare-insurers-lost-a-lot-of-money-in-2014/.

owed to those who lost money."[162] Insurers would receive only 12.5% of what they thought they would receive in 2014.[163]

The transitional reinsurance plan helps stabilize premiums in early years and reduces incentives for insurers to avoid high-cost individuals by providing reinsurance payments to individuals whose medical costs reach a threshold cost, which was $70,000 in 2015.[164] Reinsurance payments stop when the individual's costs reach $250,000.[165] The federal government will reimburse the plan for at least fifty percent of the claims cost between the threshold cost and cap in 2015.[166] Funding for the reinsurance program comes from fees levied on all health insurance plans, and HHS can adjust payments to ensure that payments do not exceed contributions collected.[167] Contributions and reimbursements from the program will decline until the program expires and allows insurers to price their premiums ten to fifteen percent lower in the new marketplace.[168]

What the cyber security insurance market needs to function in the market and what government-sponsored reinsurance offers are one and the same: lower premiums and reduction of risk.[169] The need for a temporary reinsurance program will reduce once insurers gain sufficient experience in the market.[170] Reinsurance, as best exemplified through ACA and TRIA, is a risk-shifting mechanism that reallocates risks away from the most vulnerable parties.[171] This type of risk management will facilitate the widespread availability and affordability of cyber insurance coverage in the marketplace.

Modeling cyber reinsurance after the TRIA could ensure that the government does not completely take over the risk, as insurers are still responsible for modest deductibles.[172] Also, the temporary nature of the TRIA could stimulate market solutions as opposed to the more permanent NFIP model in which the government, acting as primary insurer, sets its own premiums unrelated to risk and leaves no room for the market to develop on its own.[173] A transitional government reinsurance program would have to differ from the TRIA; however, in

162. *Id.*

163. *Id.*

164. Boothe & La Couture, *supra* note 148.

165. *Id.*

166. *Id.*

167. *Id.*

168. *Id.*

169. Mark A. Hall, *Government-Sponsored Reinsurance*, 19 ANNALS HEALTH L. 465, 469 (2010).

170. *Id.* at 473.

171. DAVID A. MOSS, WHEN ALL ELSE FAILS: GOVERNMENT AS THE ULTIMATE RISK MANAGER (2002).

172. Bruggeman et al., *Insurance Against Catastrophe: Government Stimulation of Insurance Markets for Catastrophic Events*, 43 DUKE ENVTL. L. & POL'Y F. 185, 230 (2012).

173. *Id.* at 196, 236.

that it needs to truly be temporary and not constantly renewed.[174] Because the TRIA model does not charge premiums to be eligible, the costs are borne by the taxpayers subject to recoupment.[175] This is often a criticism of the continuing nature of the program, as it only extends the burden on the public taxpayers.[176]

The danger of having the federal government charge premiums for reinsurance is that the risk of cyber insurance is still not known, and providing low premiums that do not correctly reflect the risk will leave the program in massive debt.[177] It would be wise to stick with the TRIA model of not charging premiums, since even on occasions that a premium is charged for government intervention, the premium does not actually reflect the risk.[178] The ACA does not charge premiums for its reinsurance, but requires health insurance upon which it charges fees to help reinsure the risk and lower premium prices in the new market.[179] Requiring mandatory cyber insurance on organizations is too drastic a solution and an extremely complicated undertaking that may not be the fairest solution.[180]

While the TRIA model promotes cyber insurance coverage by shifting unpredictable and catastrophic economic risks to the government, a preventive risk-reducing model must also be incorporated to avert the likelihood and magnitude of said risks in the future. The National Flood Insurance Program most closely resembles a risk prevention framework. In order to qualify for flood insurance, a community must adopt floodplain management regulations and ordinances to reduce the risk and consequences of serious flooding.[181] "Flood damage is decreased by almost $1 billion a year through community enforcement of floodplain management" requirements and buildings "constructed in agreement with NFIP building standards experience about 80% less damage."[182] The NFIP must be distinguished in that the federal government acts as a primary insurer rather than reinsurer.[183] In the field of cyber security, the objective is not to completely eradicate the private insurance market, but to help stabilize it until it can function on its own. The preventative idea of the NFIP, however, could be incorporated

174. Katz, *supra* note 130.

175. *Id.*

176. *Id.*

177. Bruggeman et al., *supra* note 172, at 202, 240.

178. *Id.* at 238.

179. Boothe & La Couture, *supra* note 148.

180. Debra Shinder, *Cyber-Insurance: Is It Necessary? Should It Be Mandatory?* GFI BLOG (Dec. 4, 2014), http://www.gfi.com/blog/cyber-insurance-is-it-necessary-should-it-be-mandatory/ (last visited Nov. 29, 2017).

181. NAT'L FLOOD INS. PROGRAM, ABOUT THE NATIONAL FLOOD INSURANCE PROGRAM: MAKING COMMUNITIES SAFER, https://www.floodsmart.gov/floodsmart/pages/about/making_communities_safer.jsp (last visited Nov. 29, 2017).

182. DEP'T OF ENERGY & ENV'T, FLOODPLAIN MANAGEMENT, http://doee.dc.gov/service/floodplain-management (last visited Nov. 29, 2017).

183. *Id.*

within a reinsurance framework to help cure the incentive problem in the healthcare industry.

The ideal federal program would act both as a risk shifter and risk reducer.[184] Federal reinsurance for a data breach would be triggered by a threshold amount of loss. Since most insurance coverage for cyber security currently caps at $100 to 300 million, the baseline for qualifying for federal funds should start at least around this number. The insurance industry will still be responsible for paying for a certain amount of the losses through deductibles (the amount an insurer must pay before the federal program kicks in) and copayments (the amount insurers must pay above their individual deductibles).[185] It is hard to say how long this program will be needed, but if the law must be renewed, the threshold amount of loss should become higher each time, along with the percentage of deductibles and copayments for which the insurer is responsible.[186]

However, unlike TRIA, this federal reinsurance would not kick in for any data breach that exceeds a certain amount. The insurer must be eligible for federal reinsurance to qualify. The federal government could incentivize insurers to require policyholders to comply with minimum security standards as a condition of coverage, or adoption of a framework formulated by the government. On the condition that insurers promote these preventative measures to their policyholders, they would be eligible for federal reinsurance in the event of a massive data breach. This would avoid a moral hazard problem and instead, promote risk transfer as a means of positively influencing risk-reduction behavior.[187]

B. Increased Regulation and Guidance

The federal government classifies the strengthening of cyber security and data as "one of the most important challenges we face as a Nation."[188] One of the biggest impediments to the maturation of the cyber insurance market is the scarcity of data and unknown certainty of the risk.[189] Information sharing about cyber risks and the magnitude and loss impact of actual data breaches would help accelerate the growth of the insurance market.[190] The issue with information shar-

184. MOSS, *supra* note 171.

185. INS. INFO. INST., *supra* note 128.

186. *Id.*

187. Surminski, *supra* note 117.

188. EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR HEADS OF EXECUTIVE DEP'T & AGENCIES (Oct. 30, 2015).

189. Biener et al., *supra* note 119.

190. U.S. DEP'T OF HOMELAND SECURITY, *supra* note 124.

ing is that private organizations are concerned that "voluntarily sharing information [with the government] will expose them to significant sources of potential liability."[191]

The rise of data breaches and cyber hacks has put pressure on lawmakers to address information security.[192] In October 2015, the Senate passed the Cybersecurity Information Sharing Act ("CISA") to give companies legal immunity for sharing private data with the federal government.[193] If a company gets hit with a specific type of hack, the federal government would receive an alert and immediately warn other companies and help strengthen cyber defenses.[194] Critics are concerned with provisions in the bill that allow the Department of Homeland Security to share information gathered with other government agencies, seemingly endorsing a surveillance agenda that benefits the intelligence community.[195] CISA includes privacy guards to ensure companies wipe customer specific data before handing information to the government, but there are still worries that companies, in a hurry, might not remove all patient specific data before sharing information with the government.[196]

The bill still needs to be reconciled with two information-sharing bills passed in the House, the Protecting Cyber Networks Act ("PCNA") and the National Cybersecurity Protection Advancement Act ("NCPAA"), before it becomes law.[197] The need for government direction on information sharing is crucial to heightening security defenses.[198] The difficulty will be in how to accomplish security without infringing on privacy interests.[199] To truly promote security, any legislation aimed at information sharing must be narrowly tailored to include only that information needed for securing systems, be solely used for that purpose, and clean of any identifying personal information.[200]

In addition to information sharing, there is a need for increased guidance for development of a cyber security infrastructure. The healthcare industry needs

191. Matt Flora, *Exclusive Q&A: Information Sharing from a Legal Perspective*, COMPASS CYBER SECURITY (Aug. 26, 2015), http://www.compasscyber.com/blog/exclusive-qa-information-sharing-from-a-legal-perspective/.

192. Andrea Peterson, *Senate Passes Cybersecurity Information Sharing Bill Despite Privacy Fears,* WASH. POST (Oct. 27, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/10/27/senate-passes-controversial-cybersecurity-information-sharing-legislation/.

193. *Id.*

194. *Id.*

195. *Id.*

196. *Id.*

197. Eric A. Fischer, *Cybersecurity and Information Sharing: Comparison of H.R. 1560 (PCNA and NCPAA) and S. 754 (CISA)*, CONG. RES. SERV. 1, 1 (Nov. 6, 2015).

198. *Id.*at 11.

199. *Id.*at 2.

200. Brian Krebs, *Cybersecurity Information (Over)Sharing Act?* KREBS ON SECURITY (Oct. 27, 2015), http://krebsonsecurity.com/2015/10/cybersecurity-information-oversharing-act/#more-32656.

better guidance for use and protection of health data.[201] The federal government should be involved in defining metrics and setting data security requirements, or at least minimum standards, insurers can use to qualify companies for cyber insurance policies.[202] Information sharing would only help the government better define industry standards and best practices to help organizations manage cyber security risk.[203]

In 2013, the President issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, which directed the National Institute of Standards and Technology ("NIST") to develop a framework for reducing cyber risks to critical infrastructure.[204] The result was a general framework aimed at helping organizations evaluate their current cyber security systems in order to meet certain goals and achieve a higher level of efficiency.[205] This framework is purely voluntary and broadly applicable to any industry, but it is a good start.[206]

There is potential for insurance companies to use something like the NIST framework to evaluate risk in cyber insurance policies.[207] It has been suggested that insurers score policyholders based on the safeguards or objectives outlined in the framework.[208] Based on the score given to company, the insurer could set a premium, how high the deductible should be, and how much coverage to extend.[209] This type of guidance could be useful in the federal government's role as a risk reducer, and could help create a set of standards for insurers to abide by in order to be eligible for federal reinsurance.

VI. CONCLUSION

The ongoing rise of data breaches exposed the failure of our current system to address this problem. The newly emerging cyber insurance market is not mature enough to singlehandedly manage the risks posed by data breaches. Even if

201. Mark B. McClellan, Testimony, *Improving Health Care Quality: The Path Forward*, BROOKINGS (Jun. 26, 2013), https://www.brookings.edu/testimonies/improving-health-care-quality-the-path-forward/.

202. U.S. DEP'T OF HOMELAND SECURITY, *supra* note 124.

203. NAT'L INST. OF STANDARDS & TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1, 1 (Feb. 12, 2014).

204. NAT'L INST. OF STANDARDS & TECHNOLOGY, EXECUTIVE ORDER 13636: CYBERSECURITY FRAMEWORK, http://www.nist.gov/cyberframework/.

205. *Id.*

206. Judy Greenwald, *Cyber Security Framework Unveiled*, BUS. INS. (Mar. 2, 2014), http://www.businessinsurance.com/article/20140302/NEWS07/303029976/cybersecurity-framework-unveiled.

207. Rachel King, *Companies, Seeking Common Ground on Cybersecurity, Turn to Insurers,* WALL ST. J. (Apr. 13, 2015), http://blogs.wsj.com/cio/2015/04/13/companies-seeking-common-ground-on-cybersecurity-turn-to-insurers/.

208. *Id.*

209. *Id.*

the market were capable of handling these risks, the risk-spreading nature of insurance would not provide the incentives needed to reduce the nature of risk and mitigate its damages for the future. The federal government must take on a temporary role as both risk shifter and risk reducer if it hopes to provide a meaningful, long-lasting solution to this problem. Information sharing and regulatory guidelines can help accelerate the development of the market and set uniform standards from which insurers can demand compliance from policyholders. The very role of insurance must be refocused and only the federal government can help repurpose the insurance sector to provide a system-wide solution to data breach risk.