Carrot Beats Stick: Cybersecurity Reform Through Safe Harbor Incentives

By Laurel T. Curtiss*

* J.D. Candidate, University of Iowa College of Law, 2026; B.S. Marketing & Major in Spanish, Iowa State University, 2023. I would like to thank the editorial team of the *Journal of Corporation Law* Volume 51 for their assistance. I would also like to thank my friends and family for their support.

I. INTRODUCTION

Computers captivated the medical industry long before they were widely used.[1] The appeal is clear—computers represent a method of caring for patients and tracking their data more efficiently and effectively. In 1991, the Institute of Medicine published the first document to "comprehensively examine the possibilities inherent in electronic medical records (EMRs)."[2] In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was created, providing for the establishment of the National Committee on Vital and Health Statistics (NCVHS).[3] This committee preemptively dealt with issues "related to confidentiality, security, patient and physician identifiers, and standards for computer-based patient records," which were sure to follow widespread adoption of electronic storage of medical records.[4] Soon thereafter, the committee began advocating for "a national health information infrastructure that could assure the creation of a fully interconnected system of health care networks."[5]

While this system greatly aided hospitals and healthcare facilities in providing patient support, it also opened the door to a new host of bad actors—hackers.[6] In 2015, the healthcare records of 78.8 million individuals were compromised following a data breach

1. *See generally* Edward P. Ambinder, *A History of the Shift Toward Full Computerization of Medicine*, 1 J. ONCOLOGY PRAC. 54 (2005) (describing the history of the adoption of computers and online databases in healthcare).

2. *Id.* at 54–55.

3. *Id.* at 55.

4. *Id.*

5. *Id.*

6. John Riggi, *Ransomware Attacks on Hospitals Have Changed*, AM. HOSP. ASS'N, https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed [https://perma.cc/NPG5-K22V] (describing cyber threats to hospitals, including the evolution from "[w]hat is considered to be the first ransomware attack . . . in 1989" to contemporary "ransomware gang[s]" and international state-sponsored terrorism).

at Anthem Inc.[7] And, in 2023, an average of 364,571 healthcare records were breached every day.[8] In 2024, the largest reported data breach in healthcare history was detected—a ransomware attack on Change Healthcare.[9] While the initial estimate of affected individuals totaled 100 million, the "UnitedHealth Group has publicly confirmed [since then] that the breach involved the data of approximately 190,000,000 individuals."[10]

This growing and ever-present threat to patient data has, in turn, exposed healthcare organizations to an increasing number of data privacy lawsuits.[11] Although hospitals are not misappropriating patient data, healthcare organizations are left liable to the millions of patients affected in data breaches every year.[12] This has caused considerable concern to some state legislatures, who have proposed and adopted legislation targeting this issue.[13] Every healthcare facility that is subject to a cyber-attack should not be subject to lawsuits and class actions by affected customers or patients. Under a regime that permits these lawsuits, healthcare costs will likely increase, and many hospitals may be forced to close permanently. Therefore, there must be certain minimum standards that healthcare organizations are required to follow to protect patient data.

This Note is a comparative legal analysis of the six states that passed safe harbor laws prior to 2025.[14] Part II examines the history of the healthcare industry's exposure to cyberattacks, introduces the states that have passed legislation to minimize healthcare liability following a cyberattack, and presents the actors involved in lawmaking considerations. Part III compares the available frameworks and analyzes their strengths and

7. Steve Alder, *Healthcare Data Breach Statistics*, HIPAA J. (Oct. 26, 2025), https://www.hipaajournal.com/healthcare-data-breach-statistics/ [https://perma.cc/XFS5-L2NX].

8. *Id.*

9. *Id.* (affecting nearly 2.5 times the number of patients as the Anthem attack).

10. Steve Alder, *Nebraska AG's Lawsuit Against Change Healthcare Survives Motion to Dismiss*, HIPAA J. (Nov. 17, 2025), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ [https://perma.cc/DE6K-UKVQ].

11. Jeff Lagasse, *Patients Increasingly Suing Hospitals Over Data Breaches*, HEALTHCARE FIN. (Apr. 13, 2022), https://www.healthcareitnews.com/news/patients-increasingly-suing-hospitals-over-data-breaches [https://perma.cc/YCB6-Z238] ("Fifty-eight [data breach] lawsuits were filed in 2021, with 43 of them filed against healthcare organizations, the largest percentage among all industries."). For the potential liability resulting from these lawsuits, see Dan Lohrmann, *Legal, Financial and Insurance Implications of the CrowdStrike-Microsoft Incident*, GOV'T TECH. (Aug. 4, 2024), https://www.govtech.com/blogs/lohrmann-on-cybersecurity/legal-financial-and-insurance-implications-of-the-crowdstrike-microsoft-incident [https://perma.cc/M8SN-UXFM]; *see also* Ben Leonard, *'Nobody's Immune': States Move to Limit Health Data Breach Liability*, POLITICO PRO (July 29, 2024), https://subscriber.politicopro.com/article/2024/07/nobodys-immune-states-move-to-limit-health-data-breach-liability-00169106 (on file with the *Journal of Corporation Law*) ("As hacks have become more prevalent and bad actors have grown more sophisticated, many lawmakers have sought to protect healthcare providers, arguing they can't reasonably be held responsible for every manner of attack headed their way."); Kara D. Schwee, *Red Sky at Morning: A Look at Responsible Corporate Officer Liability for Cyber Breaches*, 45 J. CORP. L. 101, 115–17 (2020) (explaining that the increasing number of cyberattacks on hospitals may lead to corporate officers being held responsible in the event of a breach).

12. *See* Alder, *supra* note 7 (showing tens of millions of individuals affected by data breaches and reporting that "hacking is now the leading cause of healthcare data breaches").

13. *See infra* Part II.B (outlining the different frameworks state legislatures have implemented to address this cyber-attacks).

14. In 2025, Texas passed S.B. 2610, "providing safe harbor protection for small and mid-sized businesses with fewer than 250 employees." *New State-Level Safe Harbor Statutes Attempt to Curb Data Breach Litigation Risks*, QUINN EMANUEL (Sep. 19, 2025), https://www.quinnemanuel.com/the-firm/publications/new-state-level-safe-harbor-statutes-attempt-to-curb-data-breach-litigation-risks/ [https://perma.cc/TCT2-XL69].

weaknesses. Part IV proposes a federally enacted statute that implements the most effective measures and applies equally to each state, preempting existing safe harbor laws and addressing concerns related to jurisdictional analysis.

II. BACKGROUND

A. History of the Healthcare Industry's Exposure to Cyberattacks

As cyberattacks become more frequent, the healthcare sector continues to get hit hard.[15] Financial gain drives these attacks; stolen health records are up to ten times more valuable than stolen credit card numbers.[16] Not only is the healthcare industry particularly vulnerable to attack,[17] but the cost of recovery post-breach is nearly three times the cost compared to other industries.[18] When reports showed a monthly 45% increase in cybersecurity attacks against healthcare entities, H.R. 7898 was signed into law to limit the liabilities health care providers could face following a cyberattack.[19]

Prior to the adoption of H.R. 7898, states had also been working to develop their own liability protections to incentivize the adoption of more robust cybersecurity frameworks.[20] Former Vice President Kamala Harris is credited with getting "the safe harbor ball rolling" in February 2016, while serving as California's attorney general.[21] Her recommendation that the state adopt "a recognized set of industry security controls" to qualify as having "reasonable security" in a company's IT infrastructure set the stage for how other states would define "reasonable security" in safe harbor statutes.[22] "[R]ecognized cybersecurity

15. *See* Alder, *supra* note 7 ("In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. [By 2023] the rate [had] more than doubled.").

16. John Riggi, *A High-Level Guide for Hospital and Health System Senior Leaders*, AM. HOSP. ASS'N https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety [https://perma.cc/9RXL-LE8R].

17. Lagasse, *supra* note 11 (explaining that the healthcare industry experiences the "largest percentage" of data breaches "among all industries").

18. Riggi, *supra* note 16 (highlighting that each stolen health care record costs about $408 to remediate compared to $148 per every stolen non-health record).

19. Check Point Research Team, *Attacks Targeting Healthcare Organizations Spike Globally as COVID-19 Cases Rise Again*, CHECK POINT (Jan. 5, 2021), https://blog.checkpoint.com/security/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/ [https://perma.cc/9YSZ-6SE5]. For a more complete discussion of the bill, see *infra* Part II.C (outlining H.R. 7898).

20. *Id.* (describing laws passed in Ohio and Nevada).

21. *Id.*

22. *Id.* (describing the report); *see generally* CAL. DEP'T OF JUST., CALIFORNIA DATA BREACH REPORT 2012–2015 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.cc/C7ES-ZWT3].

framework[s]," such as NIST[23] and HIPAA,[24] have been identified as fulfilling reasonable security requirements in most safe harbor laws that have been passed.[25]

B. Ohio as the Impetus for State Safe Harbor Laws

Six states passed cybersecurity safe harbor laws prior to 2025—Ohio, Utah, Connecticut, Iowa, Oklahoma, and Tennessee.[26] "Cybersecurity safe harbor laws are legislative acts designed to encourage businesses and organizations to take voluntary action and improve their cybersecurity."[27] The level of protection they promise, as well as the requirements healthcare organizations must follow to earn that protection, varies from state to state.[28]

In 2018, Ohio became the first state to introduce a cybersecurity safe harbor law.[29] The Ohio Data Protection Act (ODPA) provides companies with an "affirmative defense to any cause of action sounding in tort that is brought under the laws of [Ohio] . . . and that alleges that the failure to implement reasonable information security controls resulted in a data breach."[30]

"The genesis for [the ODPA] was frustration and anger that resulted from a data breach . . . at Nationwide in 2012."[31] Millions of records were compromised, resulting in five years of investigations by regulators and Attorneys General (AGs), including Ohio AG Mike DeWine.[32] Throughout settlement negotiations, one question was continuously

23. NIST, THE NIST CYBERSECURITY FRAMEWORK (CFS) 2.0 1–2 (2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [https://perma.cc/9Z32-CU3Z] (The National Institute of Standards and Technology Cybersecurity Framework (CSF) provides a "flexible framework" to be used "in conjunction with other resources").

24. *Health Insurance Portability and Accountability Act of 1996 (HIPAA*), CMS (June 20, 2023), https://security.cms.gov/learn/health-insurance-portability-and-accountability-act-1996-hipaa [https://perma.cc/HVX9-4ENU] ("The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of Protected Health Information (PHI)."). The HIPAA Security Rule, 45 C.F.R. §§ 160, 164.102–106, 164.302–318 (2025), "establishe[d] national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity."; *The Security Rule*, HHS (Oct. 20, 2022), https://www.hhs.gov/hipaa/for-professionals/security/index.html [https://perma.cc/A8JY-3LQF].

25. Joe Köller, *US Cybersecurity Safe Harbor Laws by State: All Current Legislation*, TENFOLD (Dec. 20, 2023), https://www.tenfold-security.com/en/cybersecurity-safe-harbor-laws [https://perma.cc/WE3K-4X8H] (noting that "all currently existing cybersecurity safe harbor law[s] recognize the same list of frameworks" including the "NIST Cybersecurity Framework" and the "security requirements of HIPAA/HITECH (for regulated entities)"); *see also infra* Part II.B.

26. *See infra* Part II.B.1–2.

27. Köller, *supra* note 25.

28. *See id.* (describing the state laws and notable differences between them).

29. Cynthia Brumfield, *States Enact Safe Harbor Laws Against Cyberattacks, but Demand Adoption of Cybersecurity Frameworks*, CSO (Mar. 29, 2021), https://www.csoonline.com/article/570529/states-enact-safe-harbor-laws-against-cyberattacks-but-demand-adoption-of-cybersecurity-frameworks.html [https://perma.cc/LS7E-9F62].

30. Köller, *supra* note 25 (quoting S.B. 220, 132nd Gen. Assembly, § 1354.02(D)(1) (Ohio 2018)).

31. *The State(s) of Cyber Incentives: Creative Laws Driving Better Security*, YOUTUBE at 4:05–4:16 (Aug. 22, 2022) [hereinafter *The State(s) of Cyber Incentives*], https://www.youtube.com/watch?v=3Nvyy3XHDUs [https://perma.cc/5M9J-G6E4].

32. *Id.* at 4:05–4:35, 5:25–5:40; Brian Ray, *Ohio's Data Protection Act and/as a Process-Based Approach to "Reasonable" Security*, 55 AKRON L. REV. 407, 407 (2022).

broached but never answered: what is reasonable security?[33] Although the "reasonable security" standard is required by most laws, the standard is an ever-evolving concept, making compliance difficult for businesses.[34] Recognizing a need for clarity, then AG DeWine assembled a group of "private sector experts in law, policy, and technology" to answer the following two questions: (1) what cybersecurity practices should be followed, and (2) how should businesses be made to adopt those practices?[35]

The task force returned with a novel idea; rather than trying to "scare" businesses which had not been working, they would, instead, give businesses an economic reason to improve their security.[36] The ultimate result was the ODPA, which requires compliance with "a written cybersecurity program . . . that reasonably conforms to an industry recognized cybersecurity framework" in exchange for effective immunity from civil lawsuits.[37] Although the group was not able to include relief from AG enforcement actions in the bill, the future possibility of this inclusion has not been ruled out.[38]

1. Following in Ohio's Footsteps

When Utah followed suit three years later in 2021 in the form of their Cybersecurity Affirmative Defense Act.[39] Companies that adopt a "reasonable security program" are provided with an affirmative defense to three claims: "(1) failure to implement reasonable information security controls; (2) failure to appropriately respond to a breach; and (3) failure to appropriately notify individuals whose personal information was compromised."[40]

Due to its broad protections, the Cybersecurity Affirmative Defense Act also sports a high bar to qualify for those protections.[41] For instance, the affirmative defense is not available to companies that "(1) had actual notice of the threat or hazard; (2) did not act in a reasonable amount of time to take known remedial efforts against such threat or hazard; and (3) the threat or hazard resulted in the breach," though the statute is silent on whether the burden of proof is on the plaintiff or the defendant once a cause of action is made out.[42]

In 2021, Connecticut joined Utah and Ohio, becoming the third state to adopt a cybersecurity safe harbor law.[43] The law, which was passed with a companion statute that

33. *See* Ray, *supra* note 32, at 6:00–6:30 ("As we negotiated this, I kept coming back to . . . the standard of care. What is the standard of care that you as a company or an organization have to [meet] to show that you have reasonable security?").

34. *Id.* at 6:30–7:15.

35. *Id.* at 7:30–8:03.

36. *Id.* at 16:49–18:40.

37. OHIO REV. CODE ANN. § 1354.02(A) (2018); *see also The State(s) of Cyber Incentives*, *supra* note 31, at 11:52–13:02 (explaining the statute and why the generic nature of a framework called for the language of "conformity" rather than "compliance:).

38. *The State(s) of Cyber Incentives*, *supra* note 31, at 9:52–10:33.

39. *Id.* at 13:12–13:30.

40. *Id.*

41. Köller, *supra* note 25.

42. Megan L. Brown, Kathleen E. Scott & Tawanna D. Lee, *Utah Establishes a Legal Safe Harbor for Companies That Adopt Data Security Programs*, WILEY (Apr. 2021), https://www.wiley.law/newsletter-April-2021-PIF-Utah-Establishes-a-Legal-Safe-Harbor-for-Companies-That-Adopt-Data-Security-Programs [https://perma.cc/2PAK-F47Q].

43. Köller, *supra* note 25 ("Connecticut's safe harbor law, formally known as An Act Incentivizing the Adoption of Cybersecurity Standards for Businesses (HB 6607), was signed into law on July 6, 2021 and went into effect on October 1, 2021.").

outlined enhanced requirements for cybersecurity protection, "provides a layer of protection to businesses against lawsuits brought against them seeking punitive damages for data breaches."[44]

The protection is narrower than that of Utah's, protecting companies only from allegations that the breach was caused by "a failure to implement reasonable cybersecurity controls."[45] Additionally, the Act does not provide a safe harbor to businesses that were grossly negligent or engaged in "wil[l]ful and wanton conduct."[46]

2. Later Adopters

Iowa's Act Relating to Affirmative Defenses for Entities Using Cybersecurity Programs, which went into effect in 2023, requires entities to follow a "written cybersecurity program that contains administrative, technical, operational, and physical safeguards for the protection of both personal information and restricted information" to qualify for its protection.[47]

The Act differs from its predecessors in that it covers breaches of restricted information as well as personal information and adds specificity to the "appropriate scale" consideration seen in most other laws.[48] The "scope of a program 'is appropriate if the cost to operate [it] is no less than the covered entity's most recently calculated maximum probably loss value.'"[49]

Oklahoma's Hospital Cybersecurity Protection Act, which also became effective in 2023,[50] provides an affirmative defense to Oklahoma hospitals if their "cybersecurity program reasonably conforms to industry-recognized frameworks" considering the scope of the organization.[51] Oklahoma is the only state that has specifically addressed its cybersecurity safe harbor act for hospitals rather than businesses in general.[52]

Lastly, in May of 2023, Tennessee Governor Bill Lee signed the Tennessee Information Protection Act (TIPA) into law, which took effect on July 1, 2025.[53] By doing so, Tennessee became the "first state to provide an explicit affirmative defense provision within its comprehensive privacy law . . . if the [parties controlling and processing

44. *Connecticut Enhances Data Privacy Laws and Protects Businesses Against Punitive Damages for Data Breaches*, WSHB (Sept. 2, 2021), https://www.wshblaw.com/news-connecticut-enhances-data-privacy-laws-and-protects-businesses-against-punitive-damages-for-data-breaches [https://perma.cc/Q4LU-97ZA].

45. Köller, *supra* note 25 (quoting H.B. 6607, 2021 Gen. Assemb., § 1(5)(b) (Conn. 2021)).

46. *Id.* (quoting H.B. 6607, 2021 Gen. Assemb., § 1(5)(b) (Conn. 2021)).

47. *Id.* (quoting H. File 553, 90th Gen. Assemb., 1st Sess., § 2(1) (Iowa 2023)).

48. *Id.*

49. *Id.* (quoting H. File 553, 90th Gen. Assemb., § 2(c)(3) (Iowa 2023)).

50. H.B. 2790, 59th Legis., 1st Sess. (Okla. 2023).

51. Köller, *supra* note 25.

52. However, Oklahoma broadened the scope of its safe harbor protection to all entities that use "reasonable safeguards" and provide notice in accordance with the statute in January 2026. Ashden Fein et al., *Oklahoma Substantially Amends Its Data Breach Notification Statute*, COVINGTON (Aug. 1, 2025), https://www.insideprivacy.com/cybersecurity-2/oklahoma-substantially-amends-its-data-breach-notification-statute/ [https://perma.cc/N849-S8MU]. A discussion of this addition is beyond the scope of this Note.

53. Natasha G. Kohne & Joseph Hold, *Tennessee Information Protection Act: What Businesses Need to Know*, AKIN GUMP (Aug. 8, 2023), https://www.akingump.com/en/insights/blogs/ag-data-dive/tennessee-information-protection-act-what-businesses-need-to-know [https://perma.cc/J3AB-GKC4].

personal data] create[], maintain[] and compl[y] with a written privacy policy that 'reasonably conforms' to the NIST Privacy Framework . . . ."[54]

Following the passage of this Act, Tennessee took an additional step by passing the Class Action Safe Harbor Act in May 2024, designed to "raise[] the liability standards for class action lawsuits . . . ."[55] The passing of the Class Action Safe Harbor Act was "[p]rompted by the escalating cost of these class action data breach litigations and the numerous headline-grabbing cyberattacks, particularly those in the healthcare industry."[56] Absent willful and wanton misconduct or gross negligence on the part of the business, "[u]nder the new law, companies are not liable in class action suits that arise from a 'cybersecurity event.'"[57] Notably, this protection "is not triggered by having a data [privacy] program."[58] Although Tennessee presents a unique approach in that it specifically exempts private hospitals from class action suit absent "willful and wanton misconduct or gross negligence,"[59] the brevity of the law and the narrowness of the protection make an analysis of Tennessee's law beyond the scope of this Note.

C. Federal Safe Harbor Laws

The United States Government placed its sights on providing nationwide protection to healthcare organizations regarding federal causes of action. In 2020, an amendment to the HITECH Act requiring the Department of Health and Human Services (HHS) to "incentivize best practice security for meeting HIPAA requirements" was easily passed by the House Energy and Commerce Committee[60] and unanimously passed by the Senate shortly thereafter.[61] The proposed legislation was lauded by health companies and providers tired of the severe penalties levelled against them as victims of cyberattacks "in spite of their well-resourced programs that employ industry best cybersecurity practices."[62]

On January 5, 2021, H.R. 7898 was signed into law by President Donald Trump.[63] The bill, also known as the HIPAA Safe Harbor Act,[64] is designed to limit the liabilities

54. *Id.*

55. Robb S. Harvey, Todd Ryan Hambidge & Shardul Desai, *New Tennessee Law Creates Heightened Liability Requirement for Class Action Data Breach Lawsuits*, HOLLAND & KNIGHT (June 27, 2024), https://www.hklaw.com/en/insights/publications/2024/06/new-tennessee-law-creates-heightened-liability-requirement [https://perma.cc/77KW-YGYT].

56. *Id.*

57. Liisa Thomas & Tracy Chau, *Impact of Tennessee's Cybersecurity Class Action Safe Harbor*, SHEPPARD MULLIN (June 25, 2024), https://www.eyeonprivacy.com/2024/06/impact-of-tennessees-cybersecurity-class-action-safe-harbor/ [https://perma.cc/6CYY-TB4Z].

58. *Id.*

59. TENN. CODE ANN. § 29-34-215(b) (2024).

60. Jessica Davis, *Health IT Groups Laud Proposed Bill Incentivizing Best Practice Security*, TECHTARGET (Dec. 15, 2020), https://www.techtarget.com/healthtechsecurity/news/366595454/Health-IT-Groups-Laud-Proposed-Bill-Incentivizing-Best-Practice-Security [https://perma.cc/ZD3D-Y9UD].

61. Jessica Davis, *HIPAA Safe Harbor Bill Becomes Law; Requires HHS to Incentivize Security*, TECHTARGET (Jan. 11, 2021), https://www.techtarget.com/healthtechsecurity/news/366595422/HIPAA-Safe-Harbor-Bill-Becomes-Law-Requires-HHS-to-Incentivize-Security [https://perma.cc/SDM6-6EM4].

62. Davis, *supra* note 60.

63. Davis, *supra* note 61.

64. Köller, *supra* note 25.

healthcare providers could face following a cyberattack, with the caveat that they must have complied with "recognized security practices" for at least a year.[65]

Despite its similar goals to those of state safe harbor laws, the HIPAA Safe Harbor Act does not provide the same legal protection, promising only "lower fines and shorter audits" from the HHS to covered entities, rather than offering an affirmative defense against breaches.[66]

In 2022, following the enactment of H.R. 7898, the American Data Privacy and Protection Act (ADPPA) was introduced to the U.S. House of Representatives.[67] This privacy bill appeared poised to upend state cybersecurity laws by explicitly preempting most state laws that contained "reasonable security language."[68] But "it failed to advance to the House or Senate."[69] Although ADPPA's attempts to "provide U.S. consumers with foundational data privacy rights, create robust oversight mechanisms and establish meaningful enforcement" failed, that does not mean this bill could not be reintroduced through "inclu[sion] in another bill in the future."[70]

D. Actors Impacted by Cyberattacks

1. Patients

Patients are one of the most important considerations for legislators addressing cybersecurity and cyberattacks in the healthcare industry. Cyberattacks can have lasting impacts on patient data, such as "electronic medical records, insurance details, and financial information."[71] Once this information is stolen, a host of issues can spring from the initial attack.[72] Because electronic medical records cannot be cancelled, patients can be left to deal with the repercussions of a cyberattack for a long time following a breach.[73]

Not only do cyberattacks pose a risk to patient privacy, but they also have the potential to impact patient safety and care delivery.[74] In a study published by the University of Minnesota, researchers discovered that, not only do ransomware attacks "decrease hospital volume by 17–26% during the initial attack week," but they also coincide with the in-hospital

65. David Dayen, *Hospital Lobbyists Fought to Cut Penalties for Cybersecurity Breaches*, AM. PROSPECT (Apr. 18, 2024), https://prospect.org/health/2024-04-18-hospital-lobbyists-fought-penalties-cybersecurity-breaches/ [https://perma.cc/TKX5-7584].

66. Köller, *supra* note 25.

67. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021–2022).

68. Jim Dempsey, *Preemption of State Cybersecurity Laws: It's Complicated*, LAWFARE (Aug. 24, 2022), https://www.lawfaremedia.org/article/preemption-state-cybersecurity-laws-its-complicated [https://perma.cc/P4EQ-TSRT].

69. Bill Tolson, *Still No Federal Data Privacy Law: What Happened to the ADPPA?*, SMARSH, https://www.smarsh.com/blog/thought-leadership/no-federal-data-privacy-law-what-happened-ADPPA [https://perma.cc/FXY3-GHLZ].

70. *Id.*

71. Tamra Durfee, *How Cyber Attacks Impact Patient Trust*, FORTIFIED HEALTH SEC., https://fortifiedhealthsecurity.com/blog/how-cyber-attacks-impact-patient-trust/ [https://perma.cc/3XD9-X3HL].

72. *See id.* (including "fraudulent insurance claims, unauthorized prescription access, or unwarranted medical procedures").

73. *Id.*

74. John Riggi, *supra* note 16 (explaining that, not only do cyberattacks leave patient records exposed, but they can also cause hospitals to lose access to medical records and devices, "such as when a ransomware virus holds them hostage," affecting patient care).

mortality rate increasing by 35–41% among admitted patients.[75] Cyberattacks can leave hospitals without full access to data and equipment or even force them to go on diversion.[76] In an industry where every second counts, a cyberattack has the potential to cripple the system and cause irreversible damage.[77]

Patients, understandably, do not want the private information they have trusted to healthcare organizations to be compromised. However, patients also want affordable, high-quality healthcare. "Since the start of 2022, the number of days cash on hand for hospitals and health systems has declined by 28.3%."[78] Although data breaches cost providers an immense amount of money, "[c]ybersecurity initiatives are also costly," and the cost greatly affects departmental budgets.[79] This could conceivably lead to increased costs for patients,[80] a group that routinely avoids seeking care due to the present state of healthcare prices.[81] While Congress is considering bills to reduce patient costs, it is likely that these reductions would "exacerbate financial challenges for hospitals and [further] threaten patients' access to quality care."[82]

In addressing this group of actors, legislatures must balance patients' competing interests of having more protection vs. paying more for healthcare. Exposing healthcare organizations to a lawsuit every time a breach occurs is sure to raise healthcare costs and have the adverse effect of making healthcare less affordable for patients. Hospitals will be forced to adjust for their ever-increasing risk of lawsuits by shifting costs to the patient.

2. The American Hospital Association

Healthcare organizations experiencing a breach are forced to pay hackers to get access to patient information back as well as pay fines and endure lawsuits from affected patients.[83] In 2022, St. Margaret's Hospital in Spring Valley, Illinois, made history as the

75. Claire McGlave, Hannah Neprash & Sayeh Nikpay, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients 1 (Oct. 4, 2023) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292.

76. Durfee, *supra* note 71 (explaining that ambulances may be diverted to other hospitals when medical devices are affected).

77. *Id.*

78. AM. HOSP. ASS'N, AMERICA'S HOSPITALS AND HEALTH SYSTEMS CONTINUE TO FACE ESCALATING OPERATIONAL COSTS AND ECONOMIC PRESSURES AS THEY CARE FOR PATIENTS AND COMMUNITIES 1 (2024), https://www.aha.org/system/files/media/file/2024/05/Americas-Hospitals-and-Health-Systems-Continue-to-Face-Escalating-Operational-Costs-and-Economic-Pressures.pdf [https://perma.cc/K34A-E3X6].

79. Calvin Hennick, *The Cost of Cybersecurity in Healthcare*, CDW https://www.cdw.com/content/cdw/en/articles/security/the-cost-of-cybersecurity-in-healthcare.html [https://perma.cc/Q5QP-9GTB].

80. *See* Rea S. Hederman Jr., *The Buckeye Institute: Higher Hospital Costs Lead to Higher Prices*, BUCKEYE INST. (May 17, 2024), https://www.buckeyeinstitute.org/research/detail/the-buckeye-institute-higher-hospital-costs-lead-to-higher-prices [https://perma.cc/WWH8-7EJQ] ("[H]ospitals ultimately pass along their capital costs to patients, employers and taxpayers.").

81. *How Many People Skip Medical Treatment Due to Healthcare Costs?*, USA FACTS (Oct. 14, 2024), https://usafacts.org/articles/how-many-people-skip-medical-treatment-due-to-healthcare-costs/ [https://perma.cc/R828-T5VV] ("In 2023, 27% of American adults skipped some form of medical treatment because they couldn't afford it.").

82. AM. HOSP. ASS'N, *supra* note 78, at 9.

83. *See, e.g.*, Andrew G. Simpson, *Hospital to Pay $65M to End Suit Over Cyberattack That Exposed Patients' Nude Photos*, INS. J. (Sept. 12, 2024), https://www.insurancejournal.com/news/east/2024/09/12/792600.htm [https://perma.cc/KX58-DJ4S] (describing a class action settlement

first healthcare provider to publicly admit that a cyberattack forced them to cease operations.[84]

The American Hospital Association (AHA) opposes legislative intervention. It has made their position clear in a letter sent to the Senate Committee on Finance;[85] this letter was in response to proposed legislation in Virginia seeking to impose minimum cybersecurity standards on healthcare organizations.[86] The letter states that the AHA "cannot support proposals for mandatory cybersecurity requirements being levied on hospitals as if they were at fault for the success of hackers in perpetrating a crime."[87]

The letter goes on to stress that these are third-party attackers and technologies putting patient information at risk and that "[n]o organization . . . is or can be immune from cyberattacks."[88] While this proposition has a certain ring of truth to it, it cannot be that healthcare organizations should not be regulated more carefully when it comes to protecting consumer data from the very real possibility of cyberattacks.

III. ANALYSIS

A. Comparing the Frameworks

Because Ohio was the first state to enact a cybersecurity safe harbor law,[89] the ODPA itself has served as a framework for the statutory language of these laws in later-adopting states.[90] There are several key provisions that these safe harbor laws tend to address: types of protected information; program design expectations; methods for determining appropriate scope; what the affirmative defense covers; what it means to reasonably conform with

with patients and employees affected by a 2023 ransomware attack for $65 million, based in part on the hospital's "refus[al] to pay the undisclosed amount of ransom demanded by the hackers"); Jonathan Reed, *Change Healthcare Attack Expected to Exceed $1 Billion in Costs*, IBM https://securityintelligence.com/news/change-healthcare-cyberattack-exceeds-1-billion-costs/ [https://perma.cc/BA3W-Q6L6] (acknowledging the "steep" legal costs that will result from the 24 class-action lawsuits resulting from the Change Healthcare ransomware attack).

84. David Dayen, *Hospital Lobbyists Fought to Cut Penalties for Cybersecurity Breaches*, AM. PROSPECT (Apr. 18, 2024), https://prospect.org/health/2024-04-18-hospital-lobbyists-fought-penalties-cybersecurity-breaches/ [https://perma.cc/2446-B9QP] ("Hollywood Presbyterian Medical Center had to pay hackers $17,000 in Bitcoin to regain access to its computer network in 2016.").

85. Letter from Richard J. Pollack, Pres. and CEO, Am. Hosp. Ass'n, to The Honorable Ron Wyden, Chairman, U.S. Senate Comm. on Fin., and The Honorable Mike Crapo, Ranking Member, U.S. Senate Comm. on Fin. (Mar. 13, 2024) [hereinafter Letter from Richard J. Pollack], https://www.aha.org/system/files/media/file/2024/03/aha-urges-more-congressional-action-to-help-providers-affected-by-change-healthcare-cyberattack--3-13-2024.pdf [https://perma.cc/5SZY-VU4W].

86. D. Howard Kass, *Change Healthcare Breach Brings New Legislation, Lawsuits*, MSSP ALERT (Mar. 27, 2024), https://www.msspalert.com/news/change-healthcare-breach-brings-new-legislation-and-class-action-lawsuits [https://perma.cc/9CJ5-8ZEK].

87. Letter from Richard J. Pollack, *supra* note 85, at 5.

88. *Id.*; Kass, *supra* note 86.

89. Brumfield, *supra* note 29.

90. *See* Jule Pattison-Gordon, *Carrot or Stick? States Try Incentives to Increase Cybersecurity*, GOV'T TECH. (June 1, 2022), https://www.govtech.com/security/carrot-or-stick-states-try-incentives-to-increase-cybersecurity (on file with the *Journal of Corporation Law*) ("Connecticut and Utah issued similarly worded policies in 2021.").

an industry recognized framework; and post-amendment compliance requirements.[91] The following sections analyze the changes made by the following states to Ohio's pioneering statute, using the ODPA's foundational language as a starting point. Utah, Connecticut, Iowa, and Oklahoma's safe harbor laws closely track the ODPA,[92] making the areas where individual state legislatures have chosen to diverge relevant to the present analysis.

1. Protected Information

a. Ohio, Connecticut, Iowa, & Oklahoma's Approach

The ODPA begins with the requirement that a business seeking an affirmative defense under the safe harbor law shall "[c]reate, maintain, and comply with a written cybersecurity program . . . for the protection of personal and restricted information . . . ."[93]

Personal information is "any information that includes an individual's name (first name or first initial and last name) in combination with [certain] data elements."[94] Restricted information, on the other hand, is "any unencrypted information that an individual or organization can reasonably use to distinguish an individual's identity."[95]

Although the inclusion of "restricted information" was not in the original draft of the ODPA, the addition served to establish that "organizations would be required to address a sufficiently broad range of sensitive information."[96] By including this category of data, the Ohio legislature ensured that pieces of information that did not qualify as personal information would still be included, given the risk that the aggregate pieces present in the event of a data breach.[97]

This approach, which was replicated by Connecticut,[98] Iowa,[99] and Oklahoma,[100] more wholly safeguards patient data than an approach that addresses the protection of only personal information.[101]

91. *See* OHIO REV. CODE ANN. §§ 1354.01–1354.05 (2018); UTAH CODE ANN. §§ 78B-4-701–706 (2021); CONN. GEN. STAT. § 42-901 (2021); IOWA CODE § 554G (2023); OKLA. STAT. tit. 18, §§ 2068–2072 (2023).

92. *See* OHIO REV. CODE ANN. §§ 1354.01–1354.05 (2018); UTAH CODE ANN. §§ 78B-4-701–706 (2021); CONN. GEN. STAT. § 42-901 (2021); IOWA CODE § 554G (2023); OKLA. STAT. tit. 18, §§ 2068–2072 (2023).

93. OHIO REV. CODE ANN. § 1354.02(A) (2018).

94. Nicholas Sollitto, *What Is the Ohio Data Protection Act (Senate Bill 220)?*, UPGUARD (Jan. 16, 2025), https://www.upguard.com/blog/ohio-senate-bill-220 [https://perma.cc/637D-9FEZ] (providing, as relevant data elements: social security numbers, driver's license numbers, state identification numbers, and financial account number or credit or debit card number (along with any necessary code to access the banking account)).

95. *Id.*

96. Ray, *supra* note 32, at 412.

97. *Id.* (explaining that data can be aggregated to personally identify someone, even if no piece of data was personally identifying).

98. CONN. GEN. STAT. § 42-901 (2024).

99. IOWA CODE §§ 554G.1–554G.4 (2023).

100. OKLA. STAT. tit. 18, §§ 2068–2072 (2023).

101. *See infra* Part III.A.2.a. (providing a more complete analysis of the implications of the lesser approach).

b. Utah's Approach

Utah chose not to include restricted information in its Act's protections.[102] These laws aim to incentivize businesses to adopt more effective cybersecurity practices.[103] Utah's decision not to include restricted information in its law's protections could allow hospitals to divert most of their cybersecurity resources to protect only personal information, while leaving restricted information vulnerable to attack.

2. The Written Cybersecurity Program

a. Ohio, Connecticut, Iowa, & Oklahoma's Approach

The ODPA requires businesses to "[c]reate, maintain, and comply with a written cybersecurity program" to be eligible for the affirmative defense.[104] The requirement that a business "comply" with their written program should be a commonsense inclusion within these safe harbor statutes. Similar reasoning is found in *Caremark* claims—it is not enough to implement adequate reporting and controls; those controls must also be properly monitored.[105]

Connecticut, Iowa, and Oklahoma each seem to agree with this sentiment, as their laws also demand actual compliance with a written cybersecurity program.[106]

b. Utah's Approach

Notably, Utah's Cybersecurity Affirmative Defense Act only demands reasonable compliance with a written cybersecurity program,[107] rather than the actual compliance demanded by Ohio, Connecticut, Iowa, and Oklahoma.[108] Although it is yet to be seen, this could indicate that, under Utah's law, hospitals that do not wholly comply with their written cybersecurity program may still be eligible for the affirmative defense.[109] But, what is the purpose of requiring a written cybersecurity program that is not followed? Proper monitoring and response to potential violations ought to be mandatory for hospitals to avail themselves of the affirmative defense afforded by these safe harbor statutes.

---

102. UTAH CODE ANN. § 78B-4-701 (2021).

103. Brumfield, *supra* note 29.

104. OHIO REV. CODE ANN. § 1354.02(A)(2) (2018).

105. *See* Stone v. Ritter, 911 A.2d 362, 370 (Del. 2006) (holding that *Caremark* liability arises when either there is no reporting system or "having implemented such a system or controls, [directors] consciously failed to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention"); *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 968 (Del. Ch. 1996).

106. CONN. GEN. STAT. § 42-901 (2024); IOWA CODE §§ 554G.2–554G.3 (2023); OKLA. STAT. tit. 18, § 2070 (2023).

107. *See* UTAH CODE ANN. § 78B-4-702(1) (2021) ("A person that creates, maintains, and reasonably complies with a written cybersecurity program . . . .").

108. CONN. GEN. STAT. § 42-901 (2024); IOWA CODE §§ 554G.2–554G.3 (2023); OKLA. STAT. tit. 18, § 2070 (2023).

109. Molly McGinnis Stine & Hannah Oswald, *'Safe Harbor' Ports in a Cybersecurity Litigation Storm*, TROUTMAN PEPPER LOCKE (Oct. 4, 2021), https://www.lockelord.com/newsandevents/publications/2021/10/safe-harbor-ports [https://perma.cc/PCM9-8MMK] ("The presence of the word 'reasonably' could give a company an opportunity to assert their 'reasonable compliance' under the Utah statute if their practices 'reasonably' deviate from their written cybersecurity protocols.").

Considering the limitations addressed in the previous section, this could mean that healthcare organizations in Utah are under no obligation to abide by their written cybersecurity protocol or protect certain patient information to secure the rights to an affirmative defense. As a result, patients could face consequences from both sides; their information will be afforded less protection than comparable laws offer, and they may have no avenue to recovery if hospitals can effectively raise the affirmative defense without affording the basic protections expected in other states. These safe harbor laws should be written with the primary goal of protecting patients. The protections healthcare organizations are afforded by these laws must be contingent on competent data protection; otherwise, the affirmative defense will become a way for the healthcare industry to evade lawsuits while shirking their responsibilities to patients.

3. Expectations

a. Ohio, Utah, Connecticut, & Oklahoma's Approach

"A covered entity's cybersecurity program shall be designed to do all of the following: (1) Protect the security and confidentiality of the information; (2) Protect against any anticipated threats . . . ; [and] (3) Protect against unauthorized access to and acquisition of the information . . . ."[110] Once again, the ODPA's language dominates the majority of cybersecurity safe harbor laws.[111] While this multi-factored approach to creating a written cybersecurity framework is clear in its objectives, the flexible approach introduced by Iowa is more in keeping with the ever-changing nature of technology.[112]

b. Iowa's Approach

In contrast to the ODPA,[113] Iowa requires that, to qualify for an affirmative defense, a covered entity's cybersecurity program shall be designed to "[c]ontinually evaluate and mitigate . . . threats"; "[p]eriodically evaluate no less than annually the maximum probable loss attainable from a data breach"; and "[c]ommunicate to any affected parties the extent of any risk posed . . . ."[114]

Iowa's emphasis on continuous monitoring is in line with the nature of technology. IT support specialists stress that cybersecurity is "an ever-evolving process" and developed programs "require[] diligence and frequent re-visiting."[115] Iowa seems most in tune with the field in which it is regulating.

It is surprising that more states have not gone the route of insisting on consistent monitoring of cybersecurity processes. These laws are a positive development in protecting

110. OHIO REV. CODE ANN. § 1354.02(B)(1)–(3) (2018).

111. *See* UTAH CODE ANN. § 78B-4-702(4)(a) (2024); CONN. GEN. STAT. § 42-901(d)(1) (2021); OKLA. STAT. tit. 18, § 2070(A)(2) (2023) (using the same language for program design expectations).

112. *See infra* Part III.A.4.c (explaining the clearer method for determining appropriate scope in Iowa's cybersecurity safe harbor law).

113. *See supra* Part III.A.2.a (outlining the ODPA's expectations for qualification for the affirmative defense).

114. IOWA CODE § 554G.2(2)(a)–(c) (2023).

115. Caurie Putnam, *Managing Cybersecurity Threats Is an Ever-Evolving Process*, ROCHESTER BUS. J. (Oct. 15, 2024), https://rbj.net/2024/10/15/managing-cybersecurity-threats-an-ever-evolving-process/ (on file with the *Journal of Corporation Law*).

patient data; however, creating a cybersecurity program should only represent half the battle. Legislatures should follow Iowa's lead by acknowledging that a reasonable cybersecurity program worthy of an affirmative defense should require more than a written policy—it should account for adjustments and internal audits that are designed to keep a given system in tune with the atmosphere it is designed to operate in.

4. Methods for Determining Appropriate Scope

a. Ohio, Utah, & Oklahoma's Approach

Legislatures have adopted differing approaches for determining whether a given cybersecurity program is appropriate in scope. The following factors for consideration outlined by the ODPA are also present in Utah and Oklahoma's safe harbor laws.[116]

> The scale and scope of a covered entity's cybersecurity program . . . is appropriate if it is based on all of the following factors: (1) The size and complexity of the covered entity; (2) The nature and scope of the activities of the covered entity; (3) The sensitivity of the information to be protected; (4) The cost and availability of tools to improve information security and reduce vulnerabilities; (5) The resources available to the covered entity.[117]

Although these laws have not yet been tested in court, the above factors are far more unwieldy and vague than the formula Iowa adopts. However, as analyzed below, the certainty afforded by Iowa's law may not be as beneficial as it would initially appear.[118]

b. Connecticut's Approach

The Connecticut law considers all but the resources available to the covered entity in its analysis of whether the scope of an entity's cybersecurity program is appropriate.[119] While this refusal to account for available resources may be beneficial to a patient in a lawsuit against a smaller hospital, given expectations will remain just as stringent for hospitals with fewer resources, this could ultimately lead to bankruptcy for those same hospitals while larger hospitals benefit.

c. Iowa's Approach

Iowa, once again, emerges as an outlier in cybersecurity law when it became the first state to affirmatively tell hospitals *when* the scope of their cybersecurity program is appropriate. Iowa's law states that "[t]he scale and scope . . . is appropriate if the cost to operate the cybersecurity program is no less than the covered entity's most recently calculated maximum probable loss value."[120] The Iowa law defines "maximum probable loss" as "the greatest damage expectation that could reasonably occur from a data breach."[121] To

116. OHIO REV. CODE ANN. § 1354.02(C) (2018); UTAH CODE ANN. § 78B-4-702(4)(c) (2021); OKLA. STAT. tit. 18, § 2070(A)(3) (2023).

117. OHIO REV. CODE ANN. § 1354.02(C) (2018).

118. *See infra* Part IV.A.3.

119. CONN. GEN. STAT. § 42-901(d) (2024).

120. IOWA CODE § 554G.2(3) (2023).

121. *Id.* § 554G.1(9).

perform the calculation, hospitals will multiply "damage expectation," or "the total value of possible damage," by "the probability that damage would occur."[122]

By taking the guesswork out of the analysis, Iowa's affirmative defense plan may reduce the burden on the judiciary and the parties. However, "[t]he most common problem in quantitative assessment is that there is not enough data to be analyzed."[123] It is not outside the realm of possibility that a crafty healthcare organization could use this model to reduce their cybersecurity investment and legal liability by relying on uncertain risk of loss data to propel their analysis.

On the other hand, applying this analysis could be frustratingly circular. A healthcare organization that pays more for their cybersecurity necessarily lowers their risk of breach. However, if the amount they are required to invest is based on what they will lose, anyway, organizations may determine that it makes more sense to take the gamble and invest in other areas. It may not be that this "pay now or pay later" situation truly incentivizes Iowa businesses to adopt more stringent cybersecurity measures, making the Iowa approach unattractive as a framework for incentivizing better patient data protection.

5. Affirmative Defense Coverage

a. Ohio, Iowa, & Oklahoma's Approach

The ODPA promises effective immunity from civil suit, making conformance with its conditions especially appealing to businesses.[124] "A covered entity that satisfies [the requirements for the protection of data] is entitled to an affirmative defense to any cause of action sounding in tort . . . that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information."[125] Once again, most cybersecurity safe harbor laws, following the trend, conform to ODPA's basic coverage plan.[126] Connecticut's and Utah's laws, on the other hand, depart from the ODPA and represent two ends of the incentive spectrum.[127]

b. Utah's Approach

Under Utah's approach, the affirmative defense is also applicable to breach of contract allegations relating to "fail[ure] to appropriately notify" and "fail[ure] to appropriately respond" to a breach.[128] By broadening the law's protections to include more than tort claims, Utah has given healthcare organizations a much stronger incentive for adopting more robust cybersecurity practices.

122. *Id.*

123. Volkan Evrin, *Risk Assessment and Analysis Methods: Qualitative and Quantitative*, ISACA J., no. 2, 2021, at 1, 3.

124. *The State(s) of Cyber Incentives*, *supra* note 31, at 7:45–9:00.

125. OHIO REV. CODE ANN. § 1354.02(D) (2018).

126. IOWA CODE § 554G.2(4)(a) (2023); OHIO REV. CODE ANN. § 1354.02(D) (2018); OKLA. STAT. tit. 18, § 2070(B) (2023) (limiting the affirmative defense to tort claims).

127. *See infra* Part III.A.5.c (outlining Connecticut's and Utah's differing coverage availability).

128. UTAH CODE ANN. § 78B-4-702(2)–(3) (2024).

Utah includes an important exception to qualify for its law's benefits—a notice exception;[129] this seems a natural inclusion. The purpose of these laws is to protect consumer/patient data.[130] Giving an affirmative defense to a company that knew that data was in danger and still did nothing seems to be directly contradictory to legislative intent.

c. Connecticut's Approach

Connecticut takes the opposite approach to Utah. Conformance with Connecticut's strict cybersecurity requirements does not afford businesses the affirmative defense that others do—it merely triggers a right not to be assessed punitive damages.[131] Whether Connecticut's law incentivizes businesses to adopt better cybersecurity practices remains to be seen. The extremely limited benefits afforded to healthcare organizations by the law may lead hospitals to conclude that their efforts may not be adequately protected.

Like Utah, Connecticut includes an important exception to qualify for its law's benefits. H.B. 6607 keeps punitive damages on the table if a failure to implement reasonable cybersecurity controls "was the result of gross negligence or wil[l]ful or wanton conduct."[132] Connecticut's exception seems designed to further disincentivize businesses from taking advantage of its law at all, making it a poor framework to follow in future safe harbor laws. Although the point of these laws is to incentivize businesses to better protect patient data, a balance that must be struck—the affirmative defense which incentivizes the implementation of more robust cybersecurity protections must also make financial sense for organizations to invest in.

6. Reasonable Conformance

a. Ohio, Connecticut, Iowa, & Utah's Approach

"A covered entity's cybersecurity program . . . reasonably conforms to an industry recognized cybersecurity framework" if the cybersecurity program "reasonably conforms to the entirety of the current version of" HIPAA *or* HITECH.[133] This requirement rings true for every state safe harbor law, as it relates to healthcare organizations,[134] other than Oklahoma's Hospital Cybersecurity Protection Act.[135]

129. *Id.* § 78B-4-702(5).

130. *See, e.g.*, Brumfield, *supra* note 29 ("[T]his legislation . . . is a low cost, effective way to protect businesses and consumers from cyberattacks." (quoting Caroline Simmons, who introduced the Connecticut safe harbor bill)).

131. CONN. GEN. STAT. § 42-901(b) (2024).

132. *Id.*

133. OHIO REV. CODE ANN. § 1354.03(B)(1) (2018) (providing an alternative test for meeting the burden of conforming to a framework).

134. CONN. GEN. STAT. § 42-901(c) (2024); IOWA CODE § 554G.3(1) (2023); UTAH CODE ANN. § 78B-4-703(1)(b) (2024).

135. OKLA. STAT. tit.18, § 2071 (2023).

b. Oklahoma's Approach

As the name "Oklahoma Hospital Cybersecurity Protection Act" suggests, the law applies exclusively to hospitals, rather than the broad array of businesses that the remainder of the applicable state laws cover.[136]

Oklahoma's law largely tracks that of Ohio; however, reasonable conformance requires that a hospital's "cybersecurity program reasonably conform[] to the entirety of the current version of *both* of the following"—HIPAA *and* the Health Information Technology for Economic Clinical Health Act (HITECH).[137] While HIPAA has been law longer than HITECH, HITECH was created during the Obama administration to "address[] concerns about the electronic transmission and storage of medical records" as well as "strengthen[] existing [HIPAA] provisions and introduce[] measures for the effective enforcement of HIPAA."[138]

"The HITECH Act is important because it addresses gaps identified in the existing HIPAA Rules . . . ."[139] Since Oklahoma's law is aimed directly at hospitals, the Oklahoma legislature was able to more carefully consider the industry in which it was regulating and adjust for faults within single frameworks that other states have not identified or accounted for. For the purpose of protecting patient information, Oklahoma's law incentivizes hospitals to adopt a more comprehensive and all-encompassing cybersecurity framework than comparable state laws.

7. Post-Amendment Expectations

a. Ohio & Oklahoma's Approach

ODPA states that "[w]hen a framework . . . is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not later than one year after the effective date of the amended framework."[140] Oklahoma's law requires the same.[141] Utah, Connecticut, and Iowa all utilize slightly different approaches.[142]

b. Utah's Approach

Utah allows a more discretionary approach than ODPA for changes that may need to be made given an amendment to HIPAA. When a framework that the written cybersecurity program relies upon is amended, a hospital

136. *Id.*

137. *Id.* § 2071(1) (emphasis added).

138. *HIPAA and HITECH*, HIPAA J. https://www.hipaajournal.com/hipaa-and-hitech/ [https://perma.cc/54UE-K8WU].

139. Steve Alder, *What Is the Relationship Between HITECH, HIPAA, and Electronic Health and Medical Records?*, HIPAA J. (May. 1, 2025), https://www.hipaajournal.com/relationship-between-hitech-hipaa-electronic-health-medical-records/ [https://perma.cc/BT6C-P39L].

140. OHIO REV. CODE ANN. § 1354.03(B)(2) (2018).

141. OKLA. STAT. tit. 18, § 2071(2) (2023).

142. *See* IOWA CODE § 554G.3 (2023) (considering the timeframe the chosen framework sets out); UTAH CODE ANN. § 78B-4-703(3)(b)(i)–(iii) (2021) (outlining a more relaxed standard for compliance); CONN. GEN. STAT. § 42-901 (2021) (taking a stricter approach than ODPA).

> [S]hall reasonably conform to the amend[ment] . . . in a reasonable amount of time, taking into consideration the urgency of the amendment in terms of: (i) risks to the security of personal information; (ii) the cost and effort of complying with the amended regulation; and (iii) any other relevant factor.[143]

By taking the cost of adoption into consideration, Utah gives healthcare organizations leeway to argue they have done enough; however, the courts who will be applying these laws will be left with some uncertainty. This uncertainty could lead to an increase in transaction costs for both patients and hospitals, over-complicating the analysis and making it more adversarial and expensive.

c. Connecticut's Approach

In stark contrast to Utah, Connecticut organizations are required to conform to amended cybersecurity framework requirements "not later than six months [post-amendment]" to qualify for protection from punitive damages.[144] Connecticut boasts far tighter and less forgiving requirements than ODPA in exchange for the singular benefit of exemption from punitive damages.[145] It remains difficult to see how Connecticut businesses will be incentivized to adopt conforming cybersecurity standards given the limited benefits and demanding standards Connecticut's law provides. Certain hospitals, specifically nonprofits and smaller organizations, may find this requirement impossible to comply with regardless of their intentions. Implementing a too-short time horizon for updates could deter organizations from even attempting to update their cybersecurity systems in the first place.

d. Iowa's Approach

When the legal cybersecurity framework the business is relying on is amended, Iowa's law brings in, for the first time, the timeframe the relied-upon framework itself sets out.[146] However, it still requires organizations to respond to amendments "no . . . later than one year after the effective date."[147] This approach has the potential to be even more limiting than the baseline one-year requirement advanced by the ODPA to smaller hospitals and businesses that may not have the resources to make the necessary updates in such a short timeframe if relied-upon frameworks choose shorter timelines for implementation.

B. The Carrot or the Stick? Which is Better & Other Concerns

According to Tony Sager, Senior Vice President and Chief Evangelist at the Center for Internet Security, these safe harbor laws provide people with an economic incentive to improve their security rather than attempting to scare them into compliance.[148] Sager asserts that the "carrot approach" is promising and points out that "governments may have

143. UTAH CODE ANN. § 78B-4-703(3)(b)(i)–(iii) (2021).

144. CONN. GEN. STAT. § 42-901(c)(B) (2021).

145. *Compare* CONN. GEN. STAT. § 42-901 (2021), *with* OHIO REV. CODE ANN. §§ 1354.01–1354.05 (2018).

146. IOWA CODE § 554G.3 (2023).

147. *Id.* § 554G.3(2)(f)(2).

148. *The State(s) of Cyber Incentives*, *supra* note 31, at 16:50–18:35, 30:00–30:54 (stating that these laws focus on incentives rather than on emotional appeals for cybersecurity and describing the value of having companies feel like they can "earn" protection rather than being "in trouble if [they] don't do it").

an easier time getting such incentive-focused policies passed than they would with regulations, which often face steep industry pushback."[149] However, the impact of these laws is yet to be seen.[150] Even though the ODPA, which was passed in 2018, has not yet been tested in court, proponents say that this does not mean these laws have no effect.[151] It is likely that cybersecurity safe harbor laws are "discouraging some parties from attempting to bring suit in the first place and may be giving businesses a greater sense of protection."[152] This sense of protection is especially important in the healthcare industry, an industry that "cybersecurity providers agree [is] . . . financially under-resourced."[153]

Although these laws are meant to incentivize the adoption of more stringent cybersecurity, the incentive safe harbors provide may not accomplish all that legislators hope they will. Critics have raised concerns that these laws will only complicate the jurisdictional analysis and increase court costs as a result.[154] It is for this reason that the team spearheading this project and aiding legislatures to develop these laws desire a "uniform standard" from the federal government for the cybersecurity standards in these safe harbor laws in play.[155] The bottom-up approach has been promising, according to Sager, but his hope is to implement change at the federal level.[156] National implementation will naturally lead to a decline in choice-of-law litigation and a decrease in court costs. The adoption and continued revision of H.R. 7898 signifies the federal government's openness to addressing this problem at a national level.[157]

IV. RECOMMENDATION

A. Key Provisions

Several key provisions that these safe harbor laws address include: types of protected information; program design expectations; methods for determining appropriate scope; what the affirmative defense covers; what it means to reasonably conform with an industry recognized framework; and post-amendment compliance requirements.[158] By taking the

149. Pattison-Gordon, *supra* note 90.

150. *See id.* ("[I]t's unclear how many companies are seeking to up their cybersecurity strategies in response to the policies.").

151. *Id.* ("[Bob] Hackett, too, said that he is unaware of Ohio's law being tested in court since its passage several years ago. But that doesn't mean the policy is without effect.").

152. *Id.* (quoting State Senator Bob Hackett, who co-sponsored the bill).

153. Alexis Kayser, *Hospitals Are Hacked, Then Sued. Is It Fair?*, NEWSWEEK (June 10, 2024), https://www.newsweek.com/hospitals-are-hacked-then-sued-it-fair-1910523 (on file with the *Journal of Corporation Law*).

154. DENNIS HIRSCH, BRIAN RAY & KEIR LAMONT, PROMOTING BETTER CYBERSECURITY 13 (2019), https://moritzlaw.osu.edu/sites/default/files/2021-12/cybersecurity-whitepaper-32819F-1.pdf [https://perma.cc/2C9P-RNE5] ("[T]he availability of the defense under Ohio law and in Ohio courts may create an incentive for both sides to forum shop and lead to increased litigation over choice-of-law and other procedural questions.").

155. *The State(s) of Cyber Incentives*, *supra* note 31, at 45:23–47:07 (proposing guidelines and grants from the federal government).

156. Pattison-Gordon, *supra* note 90.

157. *See supra* Part II.C ("On January 5, 2021, H.R. 7898 was signed into law by President Donald Trump.").

158. OHIO REV. CODE ANN. §§ 1354.01–1354.05 (2018); UTAH CODE ANN. §§ 78B-4-701–706 (2021); CONN. GEN. STAT. § 42-901 (2021); IOWA CODE §§ 554G.1–554G.4 (2023); OKLA. STAT. tit. 18, §§ 2068–2072 (2023).

most workable and effective portions from each piece of legislation, legislatures can ensure that healthcare organizations are appropriately incentivized to adopt more robust cybersecurity standards.

1. Protected Information & the Written Cybersecurity Program

To ensure patient data is properly protected, it is sensible to include *both* personal and restricted information in the requirements for qualification for the affirmative defense. Including personal and restricted information in these laws guarantees that *any* information that would make an individual identifiable to savvy hackers in the event of a data breach is accounted for and protected.[159] Neglecting to include both categories of information, as Utah has,[160] could have the adverse effect of leaving patient data open to hackers, as hospitals divert funds to ensuring that only the bare minimum is protected to secure a safe harbor.

Furthermore, actual compliance should be the standard, rather than the reasonable compliance demanded by Utah's Cybersecurity Affirmative Defense Act.[161] Creating a written cybersecurity program without needing to follow it negates the reason for the creation of these programs.[162] Courts are now acknowledging that passively monitoring an organization is not enough, especially in cases where health and safety are at risk.[163] This is a sensible development. Where health and safety are at risk, organizations should be required to take a more active role in ensuring their monitoring and compliance systems are robust. Placing a reasonableness standard on hospitals is akin to granting them a license to passively protect patient information. This directly contradicts the goals of this type of legislation,[164] and actual compliance should be demanded. A written cybersecurity program that is not followed is of no use to healthcare organizations or patients. These programs should have actionable steps that are possible for organizations to follow. Permitting organizations to remain idle after creating a cybersecurity program gives them no incentive to truly achieve cybersecurity compliance.

Healthcare organizations are, ultimately, naturally incentivized to take the path that saves them the most funds and manpower to help their own bottom line, rather than the data of their patients. Because of this reality, they should be required to protect both personal and restricted patient information under an actual compliance approach to qualify for affirmative defense protection.

2. Expectations

Continual evaluation and mitigation of threats should be intrinsically tied to these pieces of legislation. Iowa's approach, requiring organizations' cybersecurity programs to be designed to "[c]ontinually evaluate and mitigate . . . threats . . . ." and conduct

159. Ray, *supra* note 32, at 412.

160. UTAH CODE ANN. § 78B-4-701 (2024).

161. *Id.* § 78B-4-703.

162. *See generally* Brumfield, *supra* note 29 (explaining that the purposes of these acts as protecting consumer data and reducing cyberattacks).

163. Marchand v. Barnhill, 212 A.3d 805, 809, 824 (Del. 2019) (requiring specialized oversight for mission-critical operations).

164. Brumfield, *supra* note 29.

periodic evaluations,[165] far and away surpasses the remainder of the state safe harbor laws in this regard. Given the ever-changing nature of the technological landscape,[166] continual monitoring should be a requirement.

Organizations must be constantly poised to adapt to new and emerging threats to patient data and maintain protection. Hospitals should not be allowed to remain stagnant after implementing the initial cybersecurity program. Legislatures should follow Iowa's lead; technology is ever-evolving, and organizations should be required to account for the nature of the environment in which they are operating.

3. Methods for Determining Appropriate Scope

Given the differing budgetary constraints,[167] sizes, and types of healthcare organizations,[168] the factors outlined in Ohio, Utah, and Oklahoma's safe harbor laws are most appropriate. Although the Iowa model provides healthcare organizations with a more definitive answer as to when their cybersecurity system qualifies for the safe harbor,[169] it is not in the best interest of patients' continued access to healthcare.

The factors addressing resource availability and size/scope of the entity[170] are both important considerations to ensure smaller healthcare organizations remain a viable option for patients who may not have access to a larger hospital. If these factors are not taken into consideration, smaller hospitals will likely be forced to declare bankruptcy in the wake of patient lawsuits because they are unable to keep up with financial demands of cybersecurity protection. A one-size-fits-all approach cannot be implemented. Smaller hospitals should not be held to the standards of larger hospitals because they serve fewer patients and store lower quantities of sensitive information. The affirmative defense should not be structured in a way that only the largest, most well-funded healthcare organizations can utilize it. To maintain, or even improve, access to reliable healthcare for patients, legislatures should be actively working to make sure non-profit and smaller hospitals are held to the appropriate standards for their size and scale.

4. Affirmative Defense Coverage

Utah's approach of broadening its affirmative defense coverage to include both tort and breach of contract claims in exchange for the addition of a notice exception,[171] is the

165. IOWA CODE § 554G.2(2)(a) (2023).

166. Putnam, *supra* note 115 (quoting Cheryl Nelan as saying "[e]ven if you had all the budget in the world and you just did absolutely everything you could think of to lock things down and protect yourself well, things are going to evolve").

167. AM. HOSP. ASS'N, *supra* note 78, at 2 (identifying that many hospitals have been forced to divert dollars from investing in updated infrastructure to maintain access to care).

168. *See generally* AM. HOSP. ASS'N, FAST FACTS ON U.S. HOSPITALS, 2024 (2024), https://www.aha.org/system/files/media/file/2024/01/Fast-Facts-on-US-Hospitals-2024-Infographics-20240112.pdf [https://perma.cc/53PP-5G5X].

169. IOWA CODE § 554G.2(3) (2023) ("The scale and scope . . . is appropriate if the cost to operate the cybersecurity program is no less than the covered entity's most recently calculated maximum probable loss value.").

170. OHIO REV. CODE ANN. § 1354.02(C)(1), (2) & (5) (2018).

171. *See* UTAH CODE ANN. § 78B-4-702(1)(a) (2021) (granting the affirmative defense for any data breach cases so long as they are merely "brought under the laws of this state or in the courts of this state"); *id.* § 78B-4-702(5) (providing the notice exception).

appropriate combination of incentivizing cybersecurity improvements while keeping the legislative intent at the forefront.[172] By broadening the law's protections, healthcare organizations will be more likely to implement the necessary changes to ensure patient data is better protected. The inclusion of a notice requirement, on the other hand, serves to better protect patients' right to sue by ensuring that hospitals who are sloppy or careless in their data management are still held accountable. Of the available frameworks, Utah's correctly balances the need for patient privacy and cybersecurity reform with benefits to hospitals that undergo cybersecurity reform.

5. Reasonable Conformance

For the purpose of protecting patient information, cybersecurity safe harbor laws should acknowledge the pitfalls of individual frameworks and require hospitals to adopt more comprehensive and all-encompassing cybersecurity frameworks to qualify for affirmative defense coverage.

While most states follow Ohio's approach of reasonable conformance based on HIPAA compliance alone,[173] Oklahoma more appropriately addresses cybersecurity needs as they relate to hospitals.[174] By making it a requirement that hospitals reasonably conform to both HIPAA *and* HITECH,[175] the Oklahoma legislature ensured that the gaps in HIPAA are appropriately addressed, and patient data is better protected as a result.[176] This approach should be replicated in future cybersecurity frameworks.

6. Post-Amendment Expectations

Most states require an inflexible date by which healthcare organizations will be required to update their cybersecurity protocols in the event of an update to the relevant framework.[177] However, the more discretionary approach outlined by Utah makes the most sense given the differing financial, technical, and staff resources healthcare organizations may have access to.[178] By taking factors such as "the cost and effort of complying with the amended regulation" into account,[179] the law ensures organizations that are not as well-resourced still have the ability to benefit from the affirmative defense if they are responding to the changing landscape reasonably, given their resources. This is yet another aspect of a cybersecurity safe harbor law which will ensure smaller healthcare organizations are still appropriately incentivized to take steps towards ensuring patient data is adequately protected.

172. Brumfield, *supra* note 29.

173. OHIO REV. CODE ANN. § 1354.03(B)(1)(a) (2018).

174. OKLA. STAT. tit. 18, §§ 2068–2072 (2023).

175. *Id.* § 2071.

176. Alder, *supra* note 139 ("The HITECH Act is important because it addresses gaps identified in the existing HIPAA Rules . . . .").

177. OHIO REV. CODE ANN. § 1354.03(A)(2) (2018) (requiring reasonable conformance no later than one year following an update); OKLA. STAT. tit. 18, § 2071(2) (2023) (requiring reasonable conformance within one year); CONN. GEN. STAT. § 42-901(B) (2021) (requiring reasonable conformance within six months); IOWA CODE § 554G.3 (2023) (requiring reasonable conformance within the timeframe the relied-upon framework itself suggests, not to exceed one year).

178. UTAH CODE ANN. §§ 78B-4-701–705 (2021).

179. *Id.* § 78B-4-703(3)(b(ii)).

However, requiring an individualized evaluation of each healthcare organization's implementation timeline could have the undesired effect of increasing the cost of defending these actions. A more practical solution may involve adopting a longer time horizon for implementing changes, such as a year and a half. Given the time it ordinarily takes to patch and update hospital cybersecurity systems,[180] this amount of time should provide even small organizations with enough time to make the necessary updates.

B. A Nationwide Approach

To address the concern that cybersecurity safe harbor laws will only complicate the jurisdictional analysis and increase court costs as a result,[181] this affirmative defense incentive, along with the compliance framework outlined above, should be implemented at the federal level. An amendment to H.R. 7898 is the natural place for this change to be implemented.[182] While the bill is already meant to limit the liabilities health care providers could face following a cyberattack, it does not furnish the same legal protection.[183] By including the best pieces of existing cybersecurity safe harbor law frameworks to develop a national framework,[184] the top-down approach envisioned by the parties originally responsible for these laws will be fully effectuated.[185]

By updating the HIPAA Security Rule, something the Biden administration planned to do, investigations and assessments would be carried out by the Office for Civil Rights (OCR).[186] The HHS currently "administers and enforces the HIPAA Privacy, Security, and Breach Notification Rules through investigations, rulemaking, guidance, and outreach" through the OCR,[187] so they would be the office tasked with carrying out individualized assessments when the safe harbor affirmative defense was raised. However, it remains to be seen how long assessments would take and what the costs of those assessments would be. At present, complaints alleging a violation of the HIPAA Rules "must be filed within 180 days of when the person submitting the complaint knew or should have known about

180. Emily Olson, *HHS Agency Launches Program to Automate Cybersecurity at Hospitals*, HEALTHCARE DIVE (May 20, 2024), https://www.healthcaredive.com/news/healthcare-cybersecurity-arpa-h-upgrade-program/716609/ [https://perma.cc/KT7S-KFNX] ("While vendors can update consumer products in days or weeks, it might take up to a year to deploy a patch at scale in the healthcare sector, as hospitals can't keep devices offline for long and they have limited IT resources.").

181. HIRSCH, RAY & LAMONT, *supra* note 154, at 13 ("[T]he availability of the defense under Ohio law and in Ohio courts may create an incentive for both sides to forum shop and lead to increased litigation over choice-of-law and other procedural questions.").

182. *See supra* Part II.C. (outlining H.R. 7898).

183. Köller, *supra* note 25 (promising only "lower fines and shorter audits" to covered entities rather than providing an affirmative defense to breaches).

184. *See* Part IV.A. (exploring the best aspects of each state's safe harbor law).

185. *See generally The State(s) of Cyber Incentives*, *supra* note 31 (providing insight on the intentions of Kirk Herath, who was heavily involved in the creation of the ODPA).

186. HHS, HEALTHCARE SECTOR CYBERSECURITY: INTRODUCTION TO THE STRATEGY OF THE U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES 1, 5 (2024), https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf [https://perma.cc/S9GD-6X37].

187. *Id.* at 5.

the . . . violation . . . ."[188] From there, the OCR takes 180 days to investigate the breach and make its final decision.[189]

Regulators are currently looking to require cybersecurity standards for hospitals.[190] In fact, the Biden administration's hope was to allocate more than $1 billion towards helping hospitals to upgrade their cybersecurity over a ten-year period, with the eventual goal of adding "penalties for those failing to follow basic practices."[191] The safe harbor approach will likely prove more persuasive to lawmakers, as "governments may have an easier time getting such incentive-focused policies passed than they would with regulations, which often face steep industry pushback,"[192] and may serve as a way to kickstart these elevated cybersecurity goals. This is the natural next step towards ensuring patient data in the United States is better protected from cyberattacks.

C. The Corporate Actors at Play

Naturally, if the above recommendations are implemented, for-profit and non-profit hospitals will be affected differently. While both aim to provide the best possible patient care, their ability to allocate resources towards technology investments differs greatly. "Nonprofit hospitals are generally more dependent on government funding, charitable donations, and grants," whereas for-profit hospitals can "allocate more resources for technology investments."[193]

Unfortunately, in the current health-care market, "[m]any nonprofit hospitals are being sold to the for-profit sector and foregoing their philanthropic roots for greater access to capital."[194] This shift is likely only exacerbated by the exposure hospitals face regarding cyberattacks and the patient lawsuits that follow. By providing a safe harbor that takes the resources and size of the hospital into account, as Ohio, Utah, and Oklahoma do,[195] hospitals will be given the freedom to balance their exposure to risk with the protections that are most appropriate. This could, in turn, give non-profit hospitals the option of maintaining current, philanthropic operations while taking the steps to protect patient data that are feasible for their size and budget.

V. CONCLUSION

In this world of continual technological innovation, hospitals will continue to feel the effects from both sides as hackers breach their data management systems and patients sue to enforce their right to privacy. Each state that has addressed this problem with

188. *What OCR Considers During Intake & Review*, HHS (Nov. 20, 2023), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-ocr-considers-during-intake-and-review/index.html [https://perma.cc/5WU4-5B9A].

189. Lucy Galloway, *How to Successfully Handle a HIPAA Violation Investigation*, PABAU (Nov. 10, 2023), https://pabau.com/blog/hipaa-violation-investigation-guide/ [https://perma.cc/7GGW-T3LC].

190. Olson, *supra* note 180 ("Regulators want to require cybersecurity standards for hospitals too.").

191. *Id.*

192. Pattison-Gordon, *supra* note 90.

193. *Profit vs. Nonprofit Hospitals: What's the Difference?*, ACUITYMD https://www.acuitymd.com/blog/profit-vs-nonprofit-hospitals-whats-the-difference [https://perma.cc/545P-52E6].

194. Beth A. Tapper, *Nonprofit to For-Profit Hospital Conversions: Policy Implications and Alternatives*, 2004 ADVOCS.' F. 17, 17 (2004).

195. *See supra* Part III.A.4 (detailing the factors for determining appropriate scope in each state).

cybersecurity safe harbor laws can offer something to the solution. A nationwide approach to cybersecurity requirements should be enacted to both better protect patient information and protect vulnerable healthcare organizations from debilitating and frequent lawsuits.