HOSPITALS TAKEN HOSTAGE:

A NEW LEGAL FRAMEWORK FOR SECURING PUBLIC SAFETY AND CRITICAL INFRASTRUCTURE RESILIENCE IN THE FACE OF RANSOMWARE ATTACKS

Emma S. Sameth[*]

Ransomware attacks against the healthcare sector have evolved from isolated cybercrimes into systemic threats to public safety and national security, capable of disabling critical infrastructure and endangering human life. Despite the growing frequency and severity of these attacks, existing legal frameworks, including the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), the HIPAA Breach Notification Rule, and anti-money laundering regimes, remain ill-suited to address the unique risks posed by ransomware.

This Article argues that current law fails not only to deter ransomware attacks, but also to protect the public from their most dangerous consequences. Through analysis of recent cases involving ransomware attacks on hospitals and the role of cryptocurrency exchanges in facilitating such attacks, this Article demonstrates critical gaps in both incident reporting and public notification regimes. In particular, it contends that existing statutes prioritize government awareness and post hoc accountability over real-time public safety.

To address these deficiencies, this Article proposes a novel legal framework that extends cyber incident reporting into a public-facing notification system akin to emergency alert mechanisms. Specifically, it advocates for the integration of a "Cyber Emergency Alert" system—

[*] J.D. Candidate 2026, Antonin Scalia Law School at George Mason University. Thank you to my professors, mentors, and colleagues for inspiring this article, and to the federal employees that work to keep Americans safe every day

modeled on existing public warning infrastructures—to provide timely, transparent notice of ransomware attacks affecting critical services.

INTRODUCTION

In an era where digital networks underpin nearly every facet of modern life, ransomware attacks have emerged as a critical national security concern. No longer confined to the realm of financial crime, ransomware attacks are now capable of disabling hospitals, disrupting critical infrastructure, and threatening public safety on a systemic scale. These attacks exploit legal, technical, and policy gaps in cybersecurity governance, often burdening victims – including essential services like healthcare facilities – with significant damage and limited recourse. At the heart of this evolving threat is the facilitative role of cryptocurrency. Cryptocurrencies provide attackers with a largely untraceable and unregulated financial vehicle to demand and receive ransom payments – often outside the effective reach of existing financial surveillance and anti-money-laundering regimes. These attributes make cryptocurrency transactions the preferred instrument of ransomware attackers looking to operate in near secrecy.

Given the healthcare sector's disproportionately high rates of ransomware attacks and the convenience of cryptocurrency, these threats persist in the absence of effective legal standards and enforcement mechanisms. The convergence of private-sector digital weaknesses and public-sector security mandates raises concerns about the adequacy of existing legal frameworks such as the Health Insurance Portability and Accountability Act ("HIPAA"), Bank Secrecy Act ("BSA"), and forthcoming rules under the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"). As ransomware evolves from an isolated criminal enterprise to a form of asymmetric cyberwarfare, the frequency and impacts of ransomware attacks will only grow. However, U.S. law is currently ill-equipped to meet the present state of ransomware, let alone the future. This article examines the legal and strategic imperatives for rethinking how law must adapt to a threat that is both decentralized and deeply integrated into the fabric of civilian life.

Part I provides an overview of the ransomware attack process, details the healthcare sector's heightened vulnerability to ransomware attacks, and illustrates the attendant national security implications of this threat using two civil cases. Part II details and assesses the implications of the legal standards most relevant to this topic, namely CIRCIA, the HIPAA Breach Notification Rule, and the BSA. Part III explores the applications of these laws and argues that they are insufficient to remedy the public safety and national security threats posed by ransomware attacks against U.S. hospitals. Part IV proposes that CIRCIA should be amended to include a provision modeled after the HIPAA Breach Notification Rule, which can be effectively administered using the Federal Emergency Management Agency's ("FEMA") Integrated Public Alert and Warning System ("IPAWS") or a similar successor system. Part V discusses the state of cryptocurrency regulation and argues that cryptocurrency exchanges must be more highly scrutinized to deter ransomware attacks. Part VI provides further considerations for private healthcare entities subject to CIRCIA's requirements and seeks to balance the benefits of a public notification system for ransomware attacks with legitimate business interests. Part VII concludes with a discussion of remaining challenges in the legal landscape surrounding ransomware attacks

I. BACKGROUND

Critical infrastructure, like healthcare entities, are particularly attractive to ransomware attackers due to the mechanics of ransomware attacks themselves and the high-stakes nature of critical operations. This combination has made hospitals and other healthcare entities prime targets for cybercrime. Because of the extremely high stakes of healthcare systems, criminals motivated by monetary gain know they can demand huge sums of money that victims are highly incentivized to pay to resume operations. Further, healthcare systems are prime national security targets for terrorists or foreign adversaries because of the massive implications for public

safety and the feasibility of using ransom demand proceeds to fund malicious activity abroad.

A. *Ransomware Attacks, Cryptocurrency, and Critical Infrastructure*

Ransomware is a form of malicious software designed to disrupt, damage, or gain unauthorized access to computer systems, networks, or devices. The ransomware operates by encrypting files on a device, rendering them inaccessible until the victim pays the attacker's ransom demand.[2] While there are many variants of ransomware, most ransomware attacks follow a similar process: first, the perpetrator infiltrates the victim's system by infecting it with malware, which is often accomplished through phishing emails, exploitation of software vulnerabilities, or malicious downloads.[3] Then, the malware automatically encrypts the files sought by the perpetrator, rendering them completely inaccessible to the victim.[4] The encryption process prevents access to those files by restricting accessibility to those with a corresponding decryption key.[5] In order to access the locked files, the victim must pay the ransom demanded by the perpetrator in exchange for the decryption key.[6] In some cases, however, the victim never actually regains access to their data despite caving to the attacker's demands. Increasingly, some victims have also suffered "double extortion" whereby the attacker threatens the additional release, or sale on the dark web, of the victim's sensitive data

[2] CISA, *Malware, Phishing, and Ransomware*, https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware [perma.cc/K3R2-AJPB] (last accessed Dec. 8, 2024).
[3] Kurt Baker, *Introduction to Ransomware*, CROWDSTRIKE (Jan. 14, 2025), https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ [https://perma.cc/GVY9-G3DF].
[4] *Id.*
[5] *Id.*
[6] *Id.*

should they refuse to pay the ransom demand.[7] This double extortion technique is especially concerning for healthcare entities that possess sensitive patient data and protected health information ("PHI"), high value targets for cybercriminals.[8]

Usually, ransomware attackers seek payment in cryptocurrency, a type of intangible digital asset designed to serve as a medium of exchange and store of value.[9] Cryptocurrencies can be directly traded peer-to-peer or via an intermediary like a cryptocurrency exchange or even a traditional bank.[10] Exchanges serve as the platform through which cryptocurrency is bought, sold, and traded across public blockchains, which operate as ledgers recording user transactions.[11] Blockchains are essentially decentralized, shared databases maintained by a network of computers that secure crypto transactions through a complicated algorithm.[12] Transactions on the blockchain involve a sender, recipient, and digital wallets. Wallets are virtual accounts that are broadly grouped into two categories:

---

[7] Sentinel One, *What is Double Extortion Ransomware?* (last updated Aug. 11, 2025), https://www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-double-extortion/#exploring-the-use-cases-of-double-extortion (summarizing examples of double extortion ransomware attacks).

[8] *See* Elisabeth McMahon, Note, *Cybersecurity and Legal Obscurity: How Healthcare Organizations Navigate Legal Liability and Insurance Coverage in the Wake of a Cyberattack*, 27 QUINNIPIAC HEALTH L.J. 191, 201–02 (2024).

[9] *See* Jennifer Guillen, Note, *Cryptocurrency and Ransomware Attacks: Circumventing the BSA And MLCA*, 32 S. CAL. INTERDISC. L.J. 465, 469 (2023).

[10] *See id.*; *e.g.,* Hugh Son, *Morgan Stanley Close to Offering Crypto Trading Through E-Trade, Calls It 'Tip of the Iceberg,'* CNBC (Sept. 23, 2025), https://www.cnbc.com/2025/09/23/morgan-stanley-crypto-trading-e-trade-next-year.html [https://perma.cc/BF3F-W4PF].

[11] *See* Paul Tierno, CONG. RSCH. SERV., R47425, Cryptocurrency: Selected Policy Issues 15 (2023).

[12] *See* Kevin Roose, *The Latecomer's Guide to Crypto*, N.Y. TIMES (Mar. 18, 2022), https://www.nytimes.com/interactive/2022/03/18/technology/cryptocurrency-crypto-guide.html?smid=nytcore-ios-share&referringSource=articleShare&sgrp=p&pvid=C4CCB141-C9A5-4FA6-B246-F667E92F6F60#.

custodial and non-custodial. Custodial wallets are managed by a third party (i.e., an exchange), which maintains ultimate control over the private keys and the user's crypto assets.[13] Prominent examples of custodial wallets include those managed by exchanges like Binance, FTX, and Coinbase.[14] Non-custodial wallets, on the other hand, are not managed by a third party, which gives the user autonomy over the management of their assets and transactions.[15] Because no custodian exercises control over these wallets, there is no exchange platform to be regulated.[16] This feature is commonly exploited by ransomware attackers utilizing non-custodial wallets to receive ransom demands.[17]

Functionally, the wallet stores the user's cryptographically linked public and private keys.[18] These keys operate to prove a sender's crypto ownership and digitally approve user transactions on the blockchain. To initiate a transaction, the sender transmits a specified amount of crypto to the recipient's public wallet address, which is a randomly generated line of alphanumeric characters similar to a bank account number.[19] Then, the transaction is "signed" with the sender's private key, which functions like a password used to validate the

[13] Taras Zharun, *A Legal Guide to Custodial & Non-Custodial Wallets*, LEGAL NODES (Jan. 26, 2024), https://legalnodes.com/article/custodial-non-custodial-wallets [https://perma.cc/KGW2-2QXZ].

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Financial Action Task Force, *Countering Ransomware Financing* at 15 (Mar. 2023), https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Countering-Ransomware-Financing.pdf.coredownload.pdf [hereinafter *Financial Action Task Force*].

[18] *See* U.S. Dept. of Just., *Report of The Attorney General's Cyber Digital Task Force, Cryptocurrency Enforcement Framework* at 3 (Oct. 2020), https://www.justice.gov/d9/pages/attachments/2021/01/20/cryptocurrency_white_paper.final_.pdf [https://perma.cc/2RJZ-7F7X] [hereinafter *Cyber Digital Task Force Report*]; BitPay, *An In-depth Look at How Crypto Transactions Work* (Jan. 26, 2023), https://www.bitpay.com/blog/how-crypto-transactions-work#step-2-broadcasting-crypto-transactions [https://perma.cc/UQQ5-SXVX].

[19] Bitpay, *supra* note 18.

sender's identity.[20] Once the transmission is signed, it is "broadcasted" to a network of computers on the blockchain, which validates the transaction by verifying the sender's ownership and sufficiency of funds.[21] Lastly, the transaction is confirmed (i.e. added to the blockchain) using a consensus algorithm whereby network participants collectively agree that the crypto transaction is valid.[22] In some networks, this process involves "miners" who validate transactions and maintain network accountability by solving complex mathematical equations in exchange for a fixed amount of crypto.[23] In other networks, the confirmation process involves validators who essentially provide dormant crypto locked in a smart contract as collateral in exchange for the amount of crypto they "staked."[24]

Often, the victims of ransomware attacks in the U.S. are entities that serve as the backbone of our nation's security and economy. These vital entities, termed "critical infrastructure," serve important national security functions because they provide many of the essential services on which both civilian life and military readiness depend. Under the Critical Infrastructures Protection Act of 2001 ("CIPA"), the term "critical infrastructure" encompasses those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[25] President Obama's Presidential Policy Directive 21 ("PPD-21") refined this definition by designating sixteen critical infrastructure sectors, which range from critical manufacturing, energy, and information technology, to transportation systems,

[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.* (describing "proof of work" networks).
[24] *Id.* (describing "proof of stake" networks).
[25] 42 U.S.C. 5195c(e).

government facilities, and healthcare.[26] Prioritizing cybersecurity resilience across these sectors, the protection of critical infrastructure has remained a central pillar of the two most recent White House national cyber strategy policies.[27]

Because these sectors rely heavily on computer systems to provide such essential services,[28] they are less able to afford cyber disruptions and therefore especially vulnerable targets of ransomware attacks.[29] According to the Federal Bureau of Investigation's ("FBI") most recent Internet Crime Report, critical infrastructure experienced more than 1400 ransomware attacks in 2024 alone.[30] This represented a 9% increase in attack frequency from 2023, making ransomware the

---

[26] The White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience* (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/MVD5-WXA9].

[27] The White House, *National Cybersecurity Strategy* at 7 (Mar. 1, 2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/HLA6-DPRL]; The White House, *National Cyber Strategy* at 5 (Mar. 6, 2026), https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf [https://perma.cc/RF3H-TQK4].

[28] *See* Joe Mariani et al., *Incentives are key to breaking the cycle of cyberattacks on critical infrastructure*, DELOITTE (Mar. 8, 2022), https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/cyberattack-critical-infrastructure-cybersecurity.html [https://perma.cc/QMD7-GZBG] (describing how the "growing attack surface" impacts the cybersecurity of critical infrastructure); *see also* Government Accountability Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* (GAO-04-321), (May 28, 2004) ("Computers and networks essentially run the critical infrastructures that are vital to our national defense, economic security, and public health and safety.").

[29] U.S. Dep't of Just., *Comprehensive Cyber Review* at 11 (Jul. 19, 2022), https://www.justice.gov/d9/pages/attachments/2022/07/19/ccr_0.pdf [https://perma.cc/WN9J-C94K] (describing the national security threats posed by ransomware attacks).

[30] FBI, *Internet Crime Report* at 9–10 (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf [https://perma.cc/M9JL-VDW6] [hereinafter *2024 FBI Internet Crime Report*].

"most pervasive threat to critical infrastructure."[31] These are likely conservative estimates, given that FBI statistics only account for reported attacks.[32]

As Admiral Mike McConnel observed fifteen years ago, the ability of terrorist groups to acquire cyber tactics is "like nuclear proliferation, only far easier."[33] On top of billions of dollars in economic damages, ransomware attacks, and cyber-attacks more generally, against critical infrastructure entities directly harm U.S. national security. As the CISA has put it, "too many American organizations are soft targets" when it comes to cyberattacks waged by our most imminent adversaries,[34] a threat compounded by rapid advancement in adversarial cooperation.[35] While federal agencies generally believe the Peoples Republic of China ("PRC") to be the most serious cyber threat to U.S. critical infrastructure networks,[36] the nation states primarily responsible for ransomware attacks in

[31] *Id.* at 3.

[32] Naomi Hughes, Comment, *Critically Underregulated: An Analysis of The Federal Government's Shortcomings on Cybersecurity and How President Biden's Executive Order Doesn't Go Far Enough*, 74 ADMIN. L. REV. 353, 357 ("For every cybercrime reported to agencies like the FBI's Internet Crime Complaint Center, many more go unreported.").

[33] Joseph S. Nye, et al., *Securing Cyberspace: A New Domain for National Security, in* ASPEN STRATEGY GROUP POLICY BOOK SERIES 21–41 (Nicholas Burns & Jonathon Price eds., 2012).

[34] CISA, *Cybersecurity Strategic Plan (FY 2024-2026)* at 8, https://www.cisa.gov/sites/default/files/2025-01/FY2024-2026_Cybersecurity_Strategic_Plan508.pdf.

[35] ODNI, *Annual Threat Assessment* at 29–30 (Mar. 2025), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

[36] *Id.* at 11 ("The PRC remains the most active and persistent cyber threat to . . . critical infrastructure networks."); s*ee* Jen Easterly, *Strengthening America's Resilience Against the PRC Cyber Threats* (Jan. 15, 2025), https://www.cisa.gov/news-events/news/strengthening-americas-resilience-against-prc-cyber-threats [https://perma.cc/L8LU-WA7J].

particular are Russia, North Korea, and Iran.[37] Ransomware attacks financed by or perpetrated on behalf of these countries harm U.S. national security by funding malicious activity abroad, undermining U.S. military advantage, facilitating cyber espionage, and threatening public safety.[38] Moreover, by paying a ransom demand, the victim directly aids the enemy and may incentivize future attacks.[39] Cryptocurrency, as the predominant form of payment demanded by ransomware attackers, facilitates these attacks by providing the means through which attackers derive profit.[40] This trend is largely due to the ubiquitous nature and decentralized structure of crypto exchanges, perceived anonymity and convenience quick and direct payouts, the irreversibility of crypto payments, and lack of effective legal

[37] *See* CISA, *Russian GRU Targeting Western Logistics Entities and Technology Companies* (May 21, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a [https://perma.cc/45QE-2X82]; CISA, *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs* (July 25, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a [https://perma.cc/C93Z-TWVP]; CISA, *Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations* (Oct. 16, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a [https://perma.cc/QML6-MJYG].

[38] CISA, *Cyber Risk to Public Safety: Ransomware* at 1 (2020), https://www.cisa.gov/sites/default/files/2023-02/CISA%20Cyber%20Risks%20to%20Public%20Safety%20Ransomware_9.29.20%20-%20FINAL%20%28508c%29_0.pdf [https://perma.cc/CZ6F-XTS5].

[39] *See* Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, And Defending National Security*, 18 N.Y.U. J.L. & BUS. 391, 397, 399 (2022).

[40] TRM Labs, *2025 Crypto Crime Report* at 1, 15 (last accessed Mar. 21, 2026), https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/68a391925a8dd785f5430482_TRM%20-%20Report%20-%202025%20Crypto%20Crime%20Report.pdf?__hstc=19191463.75fe5f578f57d470ca5d2c78f4334137.1757520991458.1757520991458.1757520991458.1&__hssc=19191463.2.1757520991458&__hsfp=3863828579 [https://perma.cc/28LP-GCP3].

standards.[41] These characteristics of cryptocurrency transactions have made them especially attractive to cyber criminals[42] and foreign terrorist organizations ("FTO"), which are known to fund their terror campaigns by soliciting cryptocurrency donations from worldwide networks of supporters.[43]

B. *Epidemic of Ransomware Attacks Against the Healthcare Sector*

Ransomware attacks are the top cyber threat to healthcare entities.[44] According to some reports, 278 ransomware attacks against the healthcare sector were reported just in the first quarter of 2025[45] – more attacks than were reported for the entire year of 2024.[46] Because the majority of these victims do not disclose attacks, actual attack frequency is likely much higher.[47] According to FBI data from 2024, of all sixteen critical infrastructure sectors described in PPD-21, healthcare was the second most targeted sector, comprising 17% of

[41] U.S. S. Comm. on Homeland Sec. and Governmental Affs., *Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns* at 8 (2022); Nori Katagiri, *From Prepaid Cards to Bitcoin: How Did Ransomware Hackers Adopt Cryptocurrencies?* 9 JOURNAL OF CYBER POLICY 239 (2024); *Cyber Digital Task Force Report, supra* note 18, at 1.

[42] *Cyber Digital Task Force Report, supra* note 18, at 5–7.

[43] *Id.* at 6–12; Liana W. Rosen et al., CONG. RSCH. SERV, IF12537, *Terrorist Financing: Hamas and Cryptocurrency Fundraising* (2024); *see TRM Labs*, *supra* note 40, at 9–13 (detailing use of cryptocurrency by ISIS, Hamas, and Mujahideen Brigades).

[44] Health-ISAC, *2025 Health Sector Cyber Threat Landscape* at 3 (Feb. 2025), https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf [https://perma.cc/A8Q3-XNEZ].

[45] Steve Alder, *Cybersecurity Firms Report Record-Breaking Quarter for Ransomware Attacks*, THE HIPAA JOURNAL (Apr. 10, 2025), https://www.hipaajournal.com/q1-2025-ransomware-report/.

[46] *2024 FBI Internet Crime Report*, *supra* note 30, at 12 (recording 238 reports of ransomware attacks against healthcare in 2024).

[47] Alder, *supra* note 45.

attacks.[48] In 2023, healthcare was by far the hardest hit, making it the victim of about 20% of all attacks against critical infrastructure and marking a 128% increase in attack frequency from 2022 to 2023.[49]

The U.S. healthcare sector, as a subset of critical infrastructure, is a prime target of ransomware attacks due to the convergence of several interrelated factors.

Most importantly, healthcare organizations are seen as high value targets because they possess vast amounts of sensitive patient information – a valuable commodity on the black market.[50] Moreover, exploiting this information presents a myriad of new opportunities for illicit profits, as successful attackers often use stolen patient information to commit further crimes, like identity theft, and concoct

[48] *2024 FBI Internet Crime Report*, *supra* note 30, at 12.

[49] FBI, *Internet Crime Report* at 13 (2023), https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf [https://perma.cc/WF4P-ZXDL] [hereinafter *2023 FBI Internet Crime Report]*; ODNI, *Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024* (June 2024), https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf [https://perma.cc/THA8-E4F7]; ODNI, *Ransomware Attacks Surge in 2023; Attacks on Healthcare Sector Nearly Double* (Feb. 28, 2024), https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf.

[50] Craig Anderson, *How Can Healthcare Combat Ransomware and Protect Patient Data?*, B2B DAILY (Jan. 24, 2025), https://b2bdaily.com/it/how-can-healthcare-combat-ransomware-and-protect-patient-data/ [https://perma.cc/B6YA-V3KP] (reporting that, on the dark web, electronic health records sell for more than four times the price of social security details and more than twenty times the price of credit information); Microsoft, *US Healthcare at risk: Strengthening resiliency against ransomware attacks*, https://www.microsoft.com/en-us/security/security-insider/threat-landscape/US-healthcare-at-risk-strengthening-resiliency-against-ransomware-attacks [https://perma.cc/TP42-ALJ2] (last accessed Sep. 5, 2025) [hereinafter *Microsoft Report*]; Steve Alder, *Healthcare Ransomware Attacks Involve 20% of Stored Sensitive Data*, THE HIPAA JOURNAL (May 2, 2024), https://www.hipaajournal.com/healthcare-ransomware-attacks-20pc-sensitive-data/.

new social engineering schemes.[51] The sheer value of this data, and the need to control access to it, is illustrated further by the record breaking, multimillion-dollar ransom demands some healthcare entities have paid in efforts to recover patient records.[52]

Relatedly, healthcare services rely heavily on digital technology and information to function, which enlarges the exploitable "attack surface" by giving cyber attackers a universe of access points.[53] For instance, the proliferation of internet of things ("IoT") devices, which includes all internet-connected medical devices, provides attackers with tens of millions of additional exploitable entry points.[54]

Further, as a result of its underinvestment in effective cybersecurity measures, the healthcare sector relies on outdated legacy systems – technology that is "no longer produced, updated, or

[51] Anderson, *supra* note 50.

[52] *See, e.g,* Jennifer Gregory, *Change Healthcare discloses 22M ransomware payment,* SECURITY INTELLIGENCE (May 24, 2024), https://securityintelligence.com/news/change-healthcare-22-million-ransomware-payment/ [https://perma.cc/D229-EPCP] ($22 million Bitcoin payment); Katrina Manson, *Hackers Got Record Ransom of $75 Million for Cencora Breach (2*), BLOOMBERG NEWS (Sept. 18, 2024), https://news.bgov.com/white-collar-and-criminal-law/gang-got-75-million-for-cencora-hack-in-largest-known-ransom?context=search&index=1 ($75 million Bitcoin payment).

[53] *Microsoft Report*, *supra* note 50.

[54] McMahon, *supra* note 8, at 200; Greg Slabodkin, *Insulin pumps among millions of devices facing risk from newly disclosed cyber vulnerability, IBM says*, MEDTECH DIVE (Aug. 25, 2020), https://www.medtechdive.com/news/insulin-pumps-among-millions-of-iot-devices-vulnerable-to-hacker-attacks/584043/ (describing cybersecurity vulnerabilities allowing attackers to "remotely take control of insulin pumps and alter medication dosages to patients"); Heather Landi, *82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds*, FIERCE HEALTHCARE (Aug. 29, 2019), https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds (reporting that 82% of healthcare entities across five countries experienced an IoT cyber-attack over the past year).

protected due to a new, superior technology."[55] Many critical medical technologies with network capability, like ventilators, insulin pumps, and imaging systems, were not designed with cybersecurity in mind, making them easily surmountable by cyber attackers whose tactics have only grown in sophistication.[56] Relatedly, because ransomware attacks operate by denying access to data, they often fall outside the scope of cybersecurity laws, incentivizing healthcare entities to invest primarily in data confidentiality while treating availability as secondary.[57] Information security largely centers on three pillars: data confidentiality (ensuring only authorized data access), data integrity (ensuring that data can only be modified by authorized parties), and data availability (ensuring uninterrupted access to data by authorized parties).[58] Ransomware incidents are considered availability attacks because they function by denying victims the availability of their networks, systems, and data.[59] Microsoft analysis suggests that the Health Insurance Portability and Accountability Act ("HIPAA"), a federal law subjecting healthcare entities to certain cybersecurity standards in relation to protected health information ("PHI"), has resulted in prioritization of data confidentiality at the expense of data availability.[60]

And, the healthcare sector's inherent mission of prioritizing patient care makes it especially likely to pay ransoms in hopes of preventing service disruptions and avoiding reputational harm.[61]

---

[55] McMahon, *supra* note 8, at 194.

[56] Greg Slabodkin, *Legacy medical devices, growing hacker threats create perfect storm of cybersecurity risks*, MEDTECH DIVE (June 22, 2021), https://www.medtechdive.com/news/legacy-medical-devices-growing-hacker-threats-create-medtech-cyber-risks/602157/#:~:text=Deep%20Dive-,Legacy%20medical%20devices%2C%20growing%20hacker%20threats%20create%20perfect%20storm%20of,organizations%20highly%20vulnerable%20to%20attacks.

[57] Ido Kilovaty, *Availability's Law*, 88 TENN. L. REV. 69, 73, 83 (2020).

[58] *Id.* at 72, 77–78.

[59] *Id.* at 73.

[60] *Microsoft Report*, *supra* note 50.

[61] *Id.*

Representative of the healthcare sector's "reputation for paying ransoms," a Microsoft survey determined that at least 53% of targeted healthcare organizations paid a ransom demand in 2024.[62] By demonstrating willingness to pay, ceding to a ransom demand incentivizes future attacks and creates a vicious cycle that emboldens cyber attackers to strike again.

C. *The Ransomware Public Safety and National Security Threats*

Ransomware attacks against healthcare entities pose serious public safety risks and threaten U.S. national security on a systemic scale. The real-life examples below illustrate these issues and highlight their legal implications.

1. Death by Ransomware: Kidd v. Springhill Memorial Hospital

Some ransomware attacks against the healthcare sector have led to non-life-threatening physical consequences, causing affected hospitals to cancel or delay medical procedures, turn away new patients, revert to non-electronic record keeping methods, and administer incorrect medication dosages.[63] However, as a 2019 attack makes clear, ransomware attacks against hospitals are often a matter of life or death.

While most major cyber incidents gain media attention for the sheer number of people affected, the 2019 Springhill Memorial Hospital attack made headlines for its devastating effect on just two people. On July 16, 2019, expecting mother Teiranni Kidd was admitted to Springhill Memorial Hospital in Mobile, Alabama for

[62] *Id.*

[63] Helena Roland, Comment, *The Survival Of Critical Infrastructure: How Do We Stop Ransomware Attacks On Hospitals?*, 29 CATH. U. J. L. & TECH. 177, 182–84 (describing instances of ransomware attacks against hospitals).

labor induction.[64] Little did she know, the hospital had been experiencing the effects of a ransomware attack for the last seven days.[65] The hospital refused to pay the ransom demand, choosing instead to shut down its network in an effort to control the fallout.[66] As a result of the attack, critical hospital services were completely down: fetal heartbeat monitoring equipment was unavailable, fewer healthcare providers were able to monitor the fetus' condition, and patient health records were unreachable.[67] The hospital never informed Ms. Kidd of these dangerous service disruptions. Consequently, when her daughter was born with the umbilical cord wrapped around her neck, the hospital could not provide medical assistance.[68] After being born unresponsive with severe brain damage, the baby ultimately died nine months later.[69] Doctors later stated her death was preventable had the heart monitor system been accessible.[70]

In what is seemingly the first case to allege death as a consequence of a ransomware attack in the U.S., Ms. Kidd fought a legal battle against the hospital and her individual healthcare providers.[71] Among other claims in the June 4, 2020, complaint, Ms. Kidd alleged that the hospital's negligence and fraudulent non-disclosures amid the attack were a proximate cause of her child's wrongful death.[72] Notably, she argued that the hospital "planned, orchestrated, and implemented a scheme" in which it "conspiratorially

---

[64] Kevin Poulsen et al., *A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death*, WALL ST. J. (Sept. 30, 2021), https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] Poulsen et al., *supra* note 64.

[71] Amended Complaint, Kidd v. Springhill Hospitals, Inc., No. 02-CV-2020-900171 (Mobile County Cir. Ct. June 4, 2020) [hereinafter *Kidd Complaint*].

[72] *Id.* at 11.

hid, suppressed, and failed to disclose critical patient safety-related information, and further created a false, misleading, and deceptive narrative concerning the July 2019 cyberattack by deliberately failing to disclose critical factual information" to both Ms. Kidd and "the general public."[73] Had such disclosures been made, Ms. Kidd would have elected to deliver her baby at a "different and safer hospital."[74]

On top of these non-disclosures, the hospital affirmatively represented that it could safely treat patients. On the day of the attack, the hospital apparently "told media outlets that it experienced a network event but that the issue ha[d] not affected patient care."[75] The day Ms. Kidd was admitted, the hospital stated "[a]s we have worked diligently to investigate and remediate the incident, our staff has continued to safely care for our patients and will continue to provide the high quality of service that our patients deserve and expect."[76] Even after the delivery of Ms. Kidd's baby, on July 23, 2019, the hospital continued to represent that it was "maintaining excellent care" despite having "shut down [its] network to contain the incident and protect data."[77] At no time, it seems, did the hospital ever fully disclose the attack itself or the extent of damage caused. According to a cyber risk analysis report produced after the attack, "[t]here was a negative change in the clinical risk status of the [hospital's labor and deliver unit] following the ransomware attack and the loss of availability of the [electronic health record] and [obstetrical data management] systems."[78] Moreover, Ms. Kidd "was not formally or accurately

[73] *Id.* at 9–10.

[74] *Id.* at 9. As of 2025, Springhill Medical Center represents that it was named "The Best Place to Have a Baby" from 2020 to 2025. Springhill Medical Center, *Awards & Credentials*, https://springhillmedicalcenter.com/who-we-are/awards-credentials [https://perma.cc/3M9D-ZH4F] (last accessed Mar. 26, 2026).

[75] *Kidd Complaint*, *supra* note 71 at 3.

[76] *Id.*

[77] *Id.* at 4.

[78] Exhibit 87, Kidd et al. v. Springhill et al., at 64, No. 02-CV-2020-900171 (Mobile County Cir. Ct. June 4, 2020), https://bloximages.chicago2.vip.townnews.com/lagniappemobile.com/content/tncm

informed about the clinical risk status of the [hospital's labor and deliver unit]."[79] While trial was set for November 2022 and later April 29, 2024, the *Kidd* case concluded outside the courts with a settlement agreement, preventing a clear rule of law from emerging.[80]

Publicly available information surrounding the details of the attack is limited, however the perpetrator is believed to be Wizard Spider (sometimes referred to as Ryuk, the name of the ransomware variant it employs[81]), a Russia-based cybercrime group that has historically targeted U.S. hospitals.[82] From 2018 to 2021, Wizard Spider reportedly attacked at least 235 hospitals or psychiatric facilities in the U.S., prompting the Cybersecurity and Infrastructure Security Agency ("CISA") to issue an advisory regarding the "increased and imminent cybercrime threat to U.S. hospitals and healthcare providers."[83] In 2020 alone, the group reportedly amassed more than $100 million in ransom payments.[84] While Springhill Memorial

s/assets/v3/editorial/e/a6/ea6fd68a-1e08-11ef-a52e-d39caedd0d6c/6657a92a33d6e.pdf.pdf [https://perma.cc/35CS-BMNE].

[79] *Id.*

[80] Poulsen et al., *supra* note 64; Scott Johnson, *World's first ransomware death lawsuit ends with settlement*, LAGNIAPPE (Jun. 6, 2024), https://www.lagniappemobile.com/news/world-s-first-ransomware-death-lawsuit-ends-with-settlement/article_65473fca-2448-11ef-a55c-5ffc12d88b90.html.

[81] "Ryuk" is the name of a supernatural character in the *Death Note* anime series who relieves his boredom by dropping a death note into the human world, granting its finder the power to kill anyone whose name is written in it. The death note concept parallels the ransom notes that Ryuk/Wizard Spider attackers have dropped onto victim systems after encrypting their files. *See* Alexander Hanel, *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*, CROWDSTRIKE BLOG (Jan. 10, 2019), https://www.crowdstrike.com/en-us/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/#:~:text=The%20Ryuk%20ransom%20note%20is,to%20the%20BitPaymer%20ransom%20notes [https://perma.cc/V2AK-9QLV].

[82] Poulsen et al., *supra* note 64.

[83] CISA, *Ransomware Activity Targeting the Healthcare and Public Health Sector* (Nov. 2, 2020), https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a [https://perma.cc/2DQZ-F82E].

[84] Poulsen et al., *supra* note 64.

Hospital declined to reveal how much the attackers demanded, Wizard Spider's average ransom demand reportedly stands around $700,000.[85] According to the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), "U.S. law enforcement identified Ryuk as an imminent and increasing cybercrime threat to hospitals and healthcare providers in the United States" in October 2022.[86] As it stands, though, Wizard Spider is not named on OFAC's Specially Designated Nationals and Blocked Persons ("SDN") list, or any of OFAC's other sanction lists; if it were, any entity from which the group received a ransom payment could also be sanctioned or penalized by OFAC.[87]

Moreover, Wizard Spider may have worrying ties to North Korea, another frequent perpetrator of ransomware attacks against U.S. critical infrastructure.[88] For example, in 2022, OFAC sanctioned Blender.io, a virtual currency company used by North Korea to facilitate the country's malicious cyber activities and money

---

[85] *Id.*

[86] U.S. Dep't of the Treasury, *Treasury Designates Virtual Currency Money Launderer for Russian Elites and Cybercriminals* (Nov. 3, 2023), https://home.treasury.gov/news/press-releases/jy1874 [https://perma.cc/44W7-7RFZ].

[87] OFAC, *Specially Designated Nationals and Blocked Persons List*, https://www.treasury.gov/ofac/downloads/sdnlist.pdf [https://perma.cc/Y887-HNY6] (last accessed Dec.11, 2024); *see* U.S. Dep't of the Treasury, *Additional Sanctions Lists,* https://ofac.treasury.gov/other-ofac-sanctions-lists [https://perma.cc/377J-HY85] (last accessed Dec. 11, 2024); *see* Patrick Amano Dolan, Comment, *Fighting Ransomware in the Dark: The Problem with OFAC's Strict Liability Threat for Ransomware Payments*, 31 GEO. MASON L. REV. 1095, 1103–05 (2024) (discussing OFAC's approach to ransom payments and the potential consequences of paying ransom demands to sanctioned attackers).

[88] *See* U.S. Dep't of Just., *North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers* (July 25, 2024), https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals [https://perma.cc/9R4A-MABV].

laundering.[89] Uncovering a link between Ryuk and Blender.io, OFAC determined that Blender.io had facilitated the laundering of money generated by Wizard Spider's ransomware attacks.[90]

1. Cryptocurrency and *Troell*: National Security Implications of the *Kidd* Case

Another lawsuit filed in December 2024 brings to light a trove of new national security related allegations involving the Springhill Memorial ransomware attack. In *Troell v. Binance Holdings Limited*, a total of 535 plaintiffs (including Ms. Kidd) sued Binance, a global cryptocurrency exchange, for violations of the Anti-Terrorism Act ("ATA"), also known as the material support for terrorism statute.[91]

The complaint alleged that Binance provided material support for terrorism in the form of currency by "processing payments to Wizard Spider" that financed the group's activities and by "operating and maintaining" the group's cryptocurrency wallets, which were used to further the Springhill Memorial ransomware attack.[92] Effectively, the plaintiffs claimed, Binance provided the means by which Wizard Spider monetized the attack, which the complaint regards as "an act of international terrorism."[93] In response, Binance asserted that it cannot be held liable under the ATA because the Plaintiffs' allegations "boil down to lapses in its [anti-money laundering] compliance that enabled users allegedly associated with terrorists to transact on the

[89] U.S. Dep't of the Treasury, *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats* (May 6, 2022), https://home.treasury.gov/news/press-releases/jy0768 [https://perma.cc/2G25-95TQ].

[90] *Id.*

[91] Amended Complaint, Troell v. Binance Holdings Limited at 867, n.75, No.: 1:24-cv-7136 (JSR) (S.D.N.Y. Dec. 3, 2024) [hereinafter *Troell Complaint*].

[92] *Id.* at ¶ 3181.

[93] *Id.* at ¶ 3024.

Binance exchange."[94] In March of 2026, Ms. Kidd's claim was dismissed for failure to state a claim on the court's view that, even though Binance had a "general awareness of the role the Binance exchange played in terrorist financing," the claim did not rise to the level of an ATA violation for lack of a "definable nexus between Defendants' conduct and support for specific terrorist attacks."[95]

While the claim against Binance involving the Springhill Memorial attack is just one piece in a mosaic of terrorism-related allegations, this case highlights the role of crypto exchanges in the perpetuation of ransomware attacks and presents important legal questions concerning the extent to which third party intermediaries may be held liable for cyber-attacks.

II. LEGAL STANDARDS

The novel *Kidd* and *Troell* cases present numerous questions when it comes to ransomware attacks, including the scope of liability for the attacks themselves, redress for injured third parties, and broader national security implications. Two statutes that deal specifically with healthcare-related cyberattacks are the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") and the Health Insurance Portability and Accountability Act ("HIPAA") Breach Notification Rule.

A. *New Reporting Requirements Under CIRCIA*

The primary piece of legislation designed to address ransomware attacks against American critical infrastructure is CIRCIA. Signed into law in March 2022, CIRCIA requires the Cybersecurity and Infrastructure Security Agency ("CISA") to

[94] Binance Holdings Limited's Reply Memorandum of Law in Further Support of its Motion to Dismiss the Amended Complaint, Troell v. Binance Holdings Limited at 1, No.: 1:24-cv-07136-JAV (S.D.N.Y. Mar. 25, 2025).
[95] Opinion and Order at 39, ECF No. 206 (Mar. 6, 2026).

implement regulations requiring certain entities to report cyber incidents and ransomware payments to the government."[96] The final rules promulgating CIRCIA are expected to take effect in May 2026.[97]

Under CISA's notice of proposed rulemaking ("NPRM") implementing CIRCIA, the definition of "covered entity" tracks PPD-21's list of critical infrastructure sectors. As is relevant to the healthcare sector, a "covered entity" includes any entity that owns or operates (1) a hospital with at least 100 beds or (2) a critical access hospital.[98] CIRCIA requires that a "covered entity" submit a report to CISA no later than 72 hours after it "reasonably believes" that a "covered cyber incident" has occurred.[99] A "covered cyber incident" includes a cyber incident that leads to (1) "a substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network," (2) "a serious impact on the safety and resiliency of a covered entity's operational systems and processes," or (3) "a disruption of a covered entity's ability to engage in business

[96] CISA, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia [https://perma.cc/B974-8QBN] (last visited Mar. 11, 2025). This article assumes that CISA will remain operational after considerable staffing cuts and expiration of the Cybersecurity Information Sharing Act of 2015 (CISA), which is not to be confused with CISA the agency. *See* Terry Gerton, *The shutdown and CISA lapse expose new cracks in America's cyber defenses* (Oct. 8, 2025), https://federalnewsnetwork.com/cybersecurity/2025/10/the-shutdown-and-cisa-lapse-expose-new-cracks-in-americas-cyber-defenses/ [https://perma.cc/6KFF-LVQ7].

[97] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) (to be codified at 6 C.F.R. pt. 226); Tim Starks, *CISA pushes final cyber incident reporting rule to May 2026*, CYBER SCOOP (Sep. 8, 2025), https://cyberscoop.com/cisa-pushes-final-cyber-incident-reporting-rule-to-may-2026/?mod=djemCybersecruityPro&tpl=cs [https://perma.cc/UQZ8-HL9U].

[98] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), 89 Fed. Reg. 23644 (proposed Apr. 4, 2024) (to be codified at 6 C.F.R. § 226.2 (b)(11)(i)).

[99] *Id.*

or industrial operations, or deliver goods or services."[100] As the NPRM states, "patients and communities rely on [hospitals] to remain operational, including in the face of cyber incidents affecting their devices, systems, and networks to keep them functioning."

A second, less discussed measure established by CIRCIA is the Joint Ransomware Task Force ("JRTF"). The JRTF is an interagency body, co-chaired by both CISA and the FBI, charged with "coordinat[ing] an ongoing nationwide campaign against ransomware attacks."[101] It aims to "identif[y] new initiatives to effectively leverage the unique authorities and capabilities across the U.S. Government and the private sector to address ransomware threats."[102] In addition to specifically enumerated activities the JRTF is expected to carry out, CIRCIA authorizes the JRTF to coordinate "[a]ny other activities determined appropriate by the Joint Ransomware Task Force to mitigate the threat of ransomware attacks."[103]

B. *The HIPAA Breach Notification Rule*

Most healthcare entities are already subject to the HIPAA Breach Notification Rule, which requires those entities to, under certain circumstances, notify the government when patients' unsecured protected health information ("PHI") is breached.[104] Specifically, the entity must "notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed" as

[100] *Id.*
[101] 6 U.S.C. 665j.
[102] CISA, *Joint Ransomware Task Force*, https://www.cisa.gov/joint-ransomware-task-force [https://perma.cc/8QZH-VQ5R] (last visited Dec. 11, 2024).
[103] 6 U.S.C. 665j (a)(3)(H).
[104] *See* U.S. Dep't of Health & Hum. Serv's., *Breach Notification Rule*, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html [https://perma.cc/D86H-279H] (last visited Mar. 12, 2025).

a result of the breach.[105] This notification must be made "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach."[106] If the breach affects more than 500 individuals, the entity must also "notify prominent media outlets" and the Secretary of Health and Human Services ("HHS") "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach."[107] The media notice is likely to be provided "in the form of a press release to appropriate media outlets serving the affected area."[108] In the case of breaches affecting fewer than 500 individuals, the entity must only "maintain a log or other documentation of such breaches" and notify the Secretary of such breaches on an annual basis.[109]

III. CYBER ATTACKS STATUTES IN ACTION

While both CIRCIA and the HIPAA Breach Notification Rule aim to mitigate the impacts of cyber-attacks against the healthcare sector, applying these laws to the Kidd and Troell cases demonstrates that these legal frameworks do not effectively preserve public safety amidst a ransomware attack. A straightforward way to assess the effectiveness of these cyber-attack statutes is by analyzing the facts of the Kidd and Troell cases described above. It is worth noting that the HIPAA Breach Notification Rule was in effect during the Spring Hill Memorial cyberattack, while CIRCIA was not. Ultimately, the most pertinent question to ask is whether Ms. Kidd's tragedy would have been averted.

[105] 45 C.F.R. § 164.404(a)(1) (2025).
[106] 45 CFR§ 164.404(b) (2025).
[107] 45 C.F.R. § 164.406(a) (2025); 45 C.F.R. § 164.406(b) (2025); U.S. Dep't of Health and Human Serv's, *supra* note 104.
[108] U.S. Dep't of Health and Hum. Servs., *supra* note 104.
[109] 45 C.F.R. § 164.408(c) (2025).

A. *CIRCIA as Applied to the* Kidd *Case*

Under the proposed rules implementing CIRCIA, Springhill Memorial would have been required to disclose the ransomware attack before Ms. Kidd was admitted. As a threshold matter, Springhill Memorial Hospital will be a "covered entity" within CIRCIA, as it operates a hospital with more than 100 beds.[110] The ransomware attack it experienced constitutes a "covered cyber incident" because the attack led to "a substantial loss of . . . availability" of its "information system or network" given that the hospital's network was completely inaccessible for more than a week. Moreover, the attack led to a "disruption" in the hospital's ability to "deliver . . . services" given its failure to safely deliver Ms. Kidd's baby. Thus, under CIRCIA, the hospital would have been required to report the ransomware attack to CISA no later than July 12, 2019, as it was aware of the "network event" 72 hours earlier on July 9, 2019.

While Springhill Memorial's compliance with CIRCIA's reporting requirement would have provided the government with greater visibility surrounding the ransomware attack, it would not have prevented the death of Ms. Kidd's child, nor the ransomware attack itself. As it stands, CIRCIA is not revolutionary as far as preventing future cyberattacks. The law is primarily an incident identification and reporting law, the need for which has been recognized for over a decade.[111] CIRCIA leaves open a gaping hole when it comes to public disclosure of ransomware attacks with serious potential to endanger human life, leaving hospital patients like Ms.

---

[110] Springhill Med. Ctr., *Celebrating 50 Years* (Jan. 10, 2025), https://www.springhillmedicalcenter.com/news/celebrating-50-years [https://perma.cc/DD9S-PEK7] (stating that Springhill Medical Center "includes . . . [a] 270-bed hospital").

[111] John Dowdy et al., *The Cybersecurity Threat to U.S. Growth and Prosperity, in* SECURING CYBERSPACE: A NEW DOMAIN FOR NATIONAL SECURITY 129–43 (Nicholas Burns & Jonathon Price eds., 2012) (arguing for "a framework within which companies can share details of the attacks that they have faced in order to help prevent future attacks.").

Kidd with no transparency about the quality of care they will receive. This is especially pronounced given a private entity's focus on maintaining business continuity and minimizing reputational damage amid a ransomware attack.[112] While mandatory cyber-attack reporting laws may create incentives for victims to harden their cybersecurity and inform future cyber incident responses, they do not effectively deter cyber-attacks or protect victims with more than just data to lose.

B. *Interplay between CIRCIA and the HIPAA Breach Notification Rule*

While CIRCIA and the HIPAA Breach Notification Rule share commonalities as cyber reporting statutes applicable to the healthcare sector, the laws are neither individually nor in tandem sufficient to protect potential ransomware attack victims from bodily harm. On one hand, the HIPAA Breach Notification Rule is commendable because it requires notification of data breaches (from ransomware attacks or otherwise) to "prominent media outlets" if the breach involves more than 500 individuals.[113] This public notice undoubtedly serves an important patient protection function, at least in the context of incidents that solely involve data breaches. However, under that Rule, the ultimate time limit for notifying the media is 60 days after discovery of a breach.[114] This timeframe is much too late to prevent tangible damages from a ransomware attack at a hospital, especially considering that victimized hospitals may not even become aware of a breach until days or weeks after of the attack's initiation. Even if this 60-day timeframe were effective, the Rule is frequently violated by targeted entities reporting cyberattacks outside of the

[112] *See* McMahon, *supra* note 8 at 215–16 (highlighting how healthcare entities often "attempt to shield themselves from the public eye" after cyber-attacks to minimize reputational harm).

[113] 45 C.F.R. § 164.406(a) (2025).

[114] 45 C.F.R. § 164.406(b) (2025).

mandated 60-day window,[115] rendering public notice essentially useless to would-be patients. While CIRCIA's 72-hour notification window is comparatively better as far as quick incident identification and response, CIRCIA only provides for notification to the government– not the public or future hospital patients.[116]

Therefore, neither CIRCIA nor the HIPAA Breach Notification Rule provide a direct mechanism for news of the reported ransomware attack to reach potential victims in an efficient manner, creating a stark informational asymmetry with the potential to jeopardize lives. The harms suffered by Ms. Kidd and her child demonstrate how lacking this critical information can result in tragic, yet preventable, bodily harm.

IV. THE PUBLIC SAFETY THREAT: EXTENDING IDENTIFICATION INTO NOTIFICATION

To remedy the public disclosure issue left open by CIRCIA, CISA's next step should be the implementation of a cyber incident notification system designed to promptly inform the public of threats from ransomware attacks against covered entities. Using the HIPAA Breach Notification Rule and the Federal Emergency Management Agency's ("FEMA") Integrated Public Alert and Warning System ("IPAWS") as models, the rules implementing CIRCIA should require public disclosure of cyber-attacks against critical infrastructure. Within the specific context of the healthcare sector, this article argues that a ransomware attack notification system, combining the strengths of CIRCIA and the HIPAA Breach Notification Rule, would serve the

[115] Hannah T. Neprash et al., *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021* 4 (2022) (determining that, from 2016 to 2021, more than half of reported cyber-attacks against the healthcare sector were reported outside of the mandated reporting window).
[116] 6 U.S.C. § 681b(a).

interests of both hospitals and the public at large while supporting U.S. national security objectives when it comes to the ransomware threat.

A. *AMBER Alerts, But for Cyber Attacks: Protecting the Public Through Cyber Emergency Alerts*

Fusing CIRCIA's incident reporting timeframe with HIPAA's public disclosure requirement will help cure the information asymmetry problem left unaddressed by both laws.

Given that ransomware attacks against hospitals have become a true public safety threat, potentially akin to acts of terrorism, entities in the healthcare sector should be required to notify both CISA *and* the public as soon as possible and no later than 72 hours to prevent patient harm. This can be done by issuing a rule similar to the HIPAA Breach Notification Rule's media notification provision discussed in Part III (B). This rule should allow CISA to share a hospital's report of a ransomware attack with FEMA, which can then issue public warning notifications through IPAWS.[117]

IPAWS was established under Executive Order 13407 and serves as "FEMA's national system for local alerting that provides authenticated emergency and life-saving information to the public" through mobile phones, television, and radio.[118] The Integrated Public Alert and Warning System Modernization Act of 2015 provides that the Department of Homeland Security ("DHS") is to administer the

[117]As of April 2024, CISA has engaged with FEMA regarding IPAWS notifications. *See* Laura Goudreau, *CISA and FEMA IPAWS in Partnership with FCC Host Second National Meeting of Alerting Officials* (Apr. 29, 2024), https://www.cisa.gov/news-events/news/cisa-and-fema-ipaws-partnership-fcc-host-second-national-meeting-alerting-officials [https://perma.cc/6PAW-5ZGC]. However, the proposed Cyber Emergency Alert system need not actually be routed through FEMA. IPAWS could be used or could serve as a model for a separate or successor system.

[118] FEMA, *Integrated Public Alert & Warning System*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system [https://perma.cc/K5YE-GB9F] (last accessed Dec. 8, 2024).

IPAWS by providing "timely and effective warnings regarding natural disasters, acts of terrorism, and other man-made disasters or threats to public safety."[119] Currently all 50 states and Washington, D.C. use the IPAWS to issue public alerts in their respective jurisdictions.[120] As part of IPAWS, FEMA, the Federal Communications Commission ("FCC"), and cell service providers partner to provide automatic Wireless Emergency Alerts ("WEA") to mobile devices in a locally targeted area.[121] WEAs are "short emergency messages from authorized federal, state, local, tribal and territorial public alerting authorities that can be broadcast from cell towers to any WEA-enabled mobile device in a locally targeted area."[122] These alerts are designed to enhance public safety by providing actionable and "immediate, life-saving information" to users who "may be in harm's way, without the need to download an app or subscribe to a service."[123]

Historical examples of WEA issuances include shelter in place alerts sent to Boston residents as a result of the 2013 Boston Marathon Bombings, evacuation orders amidst destruction caused by hurricanes, tornadoes, and fires, and most notably AMBER alerts.[124]

---

[119] Integrated Public Alert and Warning System Modernization Act of 2015, 6 U.S.C. § 321o(a).

[120] FEMA, *IPAWS Alerting Authorities - Agencies and Organizations*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public-safety-officials/alerting-authorities/agencies-organizations [https://perma.cc/5LDQ-GNEL] (last accessed Dec. 10, 2024).

[121] FEMA, *Wireless Emergency Alerts*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/wireless-emergency-alerts [https://perma.cc/NUA6-WDHZ] (last accessed Dec. 10, 2024).

[122] *Id.*

[123] *Id; see* DHS Science & Tech. Directorate, *Wireless Emergency Alerts (WEA)* (Mar. 30, 2013), https://www.cisa.gov/sites/default/files/publications/Wireless%2BEmergency%2BAlerts%2B%28WEA%29%2BGeneral_0.pdf [https://perma.cc/V7B5-D2WS] (providing overview of the WEA system and process).

[124] CAL. STATE ASSEMB. COMM. ON UTIL'S. & COM. AND J. LEGIS. COMM. ON EMERGENCY MGMT., BRIEFING PAPER, WIRELESS EMERGENCY ALERT SYSTEM at 4 (2013), https://autl.assembly.ca.gov/sites/autl.assembly.ca.gov/files/reports/WEA%20White

Like these instances of public safety notifications, mobile phones in a hospital's geographic vicinity would receive an alert notifying the user of a ransomware attack against that hospital, giving the user a choice to avoid the facility. This new category of WEAs could be termed Cyber Emergency Alerts, reflecting the emergency implications of ransomware attacks as illustrated by the *Kidd* case.

On top of directly improving patient outcomes, the benefits of Cyber Emergency Alerts would also extend to nearby healthcare entities expected to compensate for the attacked hospital's downtime. A handful of studies examining spillover effects of ransomware attacks suggest that an attack on one hospital carries spillover effects capable of disrupting patient outcomes on a regional scale. One study of a ransomware attack against a San Diego hospital, for instance, determined that for approximately three weeks after the attack, two emergency departments within the same hospital service area experienced a daily 15% increase in mean emergency department visits and a daily 35% increase in mean ambulance arrivals.[125] Similarly, another study in California determined that hospitals hit with a ransomware attack experienced a decrease in emergency department visits and inpatient admissions for eight weeks following the attack, while nearby facilities that were not attacked saw increases in emergency department visits during the post-attack period.[126] By putting surrounding health organizations on notice of a nearby ransomware attack through a Cyber Emergency Alert, they can better

%20paper.pdf [https://perma.cc/2PW3-XYRE]; DHS Office of Inspector Gen., *FEMA's Oversight of the Integrated Public Alert & Warning System (IPAWS)* at 2 (Nov. 19, 2018), https://www.oig.dhs.gov/sites/default/files/assets/2018-11/OIG-19-08-Nov18.pdf [https://perma.cc/W6AN-U6XH].

[125] Christian Dameff et al., *Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the US*, JAMA NETWORK OPEN. 2023 at 7–8 (2023).

[126] Rahi Abouk & David Powell, *Ransomware Attacks, ED Visits and Inpatient Admissions in Targeted and Nearby Hospitals*, 331 JAMA 2129 at 2131 (2024).

prepare for the potential spillover effects on patient outcomes at their own facility.

To be sure, the proposed Cyber Emergency Alert system is statutorily authorized. As CIRCIA provides, CISA's JRTF can first exercise its broad statutory power to identify this new initiative and methods of leveraging it to more effectively counter the ransomware threat.[127] Moreover, the JRTF can leverage the resources of its co-chair organization, the FBI, to carry out CIRCIA's purpose through Cyber Emergency Alerts. The FBI has been instrumental in combatting the ransomware threat, most notably through its Internet Crime Complaint Center and Recovery Asset Team ("RAT"), positioning the Bureau as a natural partner.[128] Moreover, the proposed framework is responsive to the FCC's recent efforts to modernize and improve the efficacy of the WEA system.[129]

Relatedly, FEMA is a natural choice for intragovernmental cyber incident report sharing. While CISA itself can only publicly share anonymized information contained in incident reports, disclosure to federal entities is not subject to the same anonymization requirement.[130] Within CIRCIA, information provided to CISA as part of an incident report may be "disclosed to, retained by, and used by . . . any federal agency or department" for purposes including "responding to, or otherwise preventing or mitigating, a specific threat

[127] 6 U.S.C. 665j.

[128] *2023 FBI Internet Crime Report, supra* note 49 at 3.

[129] FCC, *FCC Announces Comment Dates for Re-examination of Emergency Alerting Systems* (last updated Feb. 24, 2026), https://www.fcc.gov/consumer-governmental-affairs/fcc-announces-comment-dates-re-examination-emergency-alerting-systems#:~:text=FCC%20Announces%20Comment%20Dates%20for%20Re%2Dexamination%20of%20Emergency%20Alerting%20Systems,-%22This%20page%20is&text=At%20its%20August%207%2C%202025,%2C%20and%20other%20accessibility%20options).&text=More%20information%20about%20EAS%20is,432%2D2275%20(videophone).

[130] 6 U.S.C. 681e(d).

of death" or "a specific threat of serious bodily harm."[131] So, CISA can disclose a covered entity's cyber incident report to FEMA, a federal agency, which can then alert the public of a ransomware threat by issuing Cyber Emergency Alerts to mobile devices in the relevant geographic area.

B. *Cyber Emergency Alerts as Applied to the* Kidd *Case*

The proposed Cyber Emergency Alert system could save people like Ms. Kidd's daughter. By empowering hospital patients through information and giving them a choice – the informed consent Ms. Kidd was not given the opportunity to provide – this system has the potential to preserve public safety on a national scale.

Hypothetically, if Springhill Memorial had complied with CIRCIA's reporting requirements, CISA would have been aware of the ransomware attack no later than July 12, 2019 – four days before Ms. Kidd presented to the hospital. Subsequently, CISA would exercise its statutory authority to share the report with FEMA, which would then promptly issue a Cyber Emergency Alert about the attack to mobile devices in the hospital's coverage zone. Under this framework, Ms. Kidd would have been notified of the week-long ransomware attack before even being admitted and therefore able to make an informed decision as to the quality of care she would receive. Not only would these affirmative disclosures have mooted many of her legal claims, but they very likely could have saved her child's life.

C. *Cyber Emergency Alerts as Applied to the Ransomware National Security Threat*

CIRCIA's reporting requirements, alone, will undoubtedly help inform the federal government's national security posture when it comes to responding to ransomware attacks against critical

[131] 6 U.S.C. 681e(a)(1)(C).

infrastructure. But the proposed Cyber Emergency Alert framework goes a step further in supporting U.S. national security objectives.

First, a ransomware attack notification system would likely incentivize critical infrastructure entities to invest in more effective cybersecurity measures. This both works to prevent cyberattacks from succeeding and serves an important deterrent function against our adversaries. By mandating public disclosure, attacked hospitals are incentivized to prioritize their cybersecurity and incident response protocols to avoid the reputational harm and legal costs associated with ransomware attacks. Ultimately, better cyber defenses help end the vicious cycle of ransomware attacks against the healthcare sector by making systems more difficult to attack in the first place.

Second, a ransomware attack notification system would bolster our economic security. Leaders from both the Biden and Trump administrations to scholars on this topic agree: economic security "is national security."[132] According to conservative estimates by the FBI, ransomware attacks cost victims $59.6 million in 2023.[133] As some cybersecurity scholars have put it, "[r]ansomware amounts to an ongoing tax by foreign gangs on U.S. governments and industry," for which "[w]e are all paying the price."[134] By incentivizing

[132] The White House, *Interim National Security Strategic Guidance* at 15 (2021), https://bidenwhitehouse.archives.gov/wp-content/uploads/2021/03/NSC-1v2.pdf; Peter Navarro, *Why Economic Security Is National Security*, REAL CLEAR POLITICS (Dec. 9, 2018), https://www.realclearpolitics.com/articles/2018/12/09/why_economic_security_is_national_security_138875.html;
see Kristen E. Eichensehr & Cathy Hwang, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549 at 611 (2023) (arguing that review of economic transactions is driven by the "increasing conflation of national security and economic security").

[133] *2023 FBI Internet Crime Report*, *supra* note 49 at 3.

[134] Alvaro Marañon & Benjamin Wittes, *Ransomware Payments and the Law*, LAWFARE (Aug. 11, 2021), https://www.lawfaremedia.org/article/ransomware-payments-and-law [https://perma.cc/6W45-YQFT]; *see* Inst. for Sec. and Tech., *Combating*

potential victims to take affirmative steps to prevent ransomware attacks, a Cyber Emergency Alert system could help break ransomware's chokehold on the American economy and therefore our national security.

Relatedly, on top of these direct monetary costs to Americans and domestic businesses, proceeds from state-sponsored ransomware attacks are often used to finance illicit activities that undermine U.S. national security in more traditional ways, as explored in Part I. By making ransomware attacks less profitable through enhanced cybersecurity measures, the second and third order harms to national security would diminish.

While implementation of the Cyber Emergency Alert system would be highly encouraging and likely save lives, it still does not address major players active in cases like *Troell* and *Kidd*: cryptocurrency exchanges.

V. THE ROLE OF CRYPTOCURRENCY EXCHANGES

In addition to utilizing the proposed Cyber Emergency Alert system, greater attention should be paid to the companies providing cryptocurrency exchanges exploited by ransomware attackers. Ransom demands are "almost exclusively" made using virtual assets and, as the *Troell* complaint illustrates, these exchanges play a critical role in the monetization, and thus perpetuation, of ransomware attacks.[135] By more tightly regulating these companies, potential

Ransomware, A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force at 9 (Sept. 2021), https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf [https://perma.cc/RT9G-F7TJ] ("Ransoms paid by private firms siphon millions of dollars toward criminal enterprise every year.") [hereinafter *Ransomware Task Force*].

[135] *Financial Action Task Force, supra* note 17 at 3; *Troell Complaint*, *supra* note 91 at 867.

ransomware attackers would be starved of, or at least more effectively prevented from accessing, a service often critical to their operations.

A. *Future Application of CIRCIA*

While the rules implementing CIRCIA are not yet in effect, they may eventually help target the intermediate crypto exchanges through which many ransom payments are made. Under CIRCIA, a covered entity must submit a ransom payment report to CISA if it pays a ransom demand as a result of a ransomware attack.[136] Within this report, the entity must include specific information including "identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack," the "ransom payment demand, including the type of virtual currency or other commodity requested," the "ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to," and the "amount of the ransom payment."[137] Given that ransom payments are typically demanded in cryptocurrency and often transmitted through exchanges, supplying the government with this identifying information will allow CISA, and other federal agencies or private firms, to more efficiently attribute the attack, locate the specific crypto wallets and exchanges used by the perpetrator, and pursue prosecution and enforcement actions.[138]

---

[136] 6 USC § 681(a)(2).

[137] 6 USC § 681b(c)(5)(C, G, H, I).

[138] Chainalysis, *35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payment*s (Feb. 5, 2025), https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/ [https://perma.cc/768B-QC6M](finding that, in 2024, "ransom funds primarily flowed through centralized exchanges (CEXs) (used to off-ramp funds), personal wallets (to hold funds), and bridges (to attempt to obscure the movement of funds."); *Financial Action Task Force*, *supra* note 17, at 25 (stating that because virtual asset service providers "act as a direct intermediary in many ransom

B. *The Agency-Driven Regulation of Crypto Exchanges*

Federal regulation of cryptocurrency exchanges remains fragmented and agency-driven, with no comprehensive statutory framework governing digital asset markets. U.S. crypto exchanges continue to fall under the jurisdiction of several federal agencies including the Treasury Department's Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC"), the Securities and Exchange Commission ("SEC"), and the Commodity Futures Trading Commission ("CFTC").

Because there is no comprehensive crypto legislation at the federal level, the ability of each of these agencies to regulate exchanges is largely dependent on how exchanges are classified under various financial statutes often originating from the 1930s and 40s. FinCEN treats exchanges as "money services businesses," requiring Bank Secrecy Act (BSA) compliance, including Know Your Customer (KYC) verification, Anti-Money Laundering (AML) program implementation, and suspicious activity reporting.[139] OFAC enforces U.S. sanctions law, requiring exchanges to block and report transactions involving sanctioned persons, entities, or wallets.[140] The SEC regulates exchanges that list tokens deemed "securities," requiring registration and enforcement of disclosure and anti-fraud rules.[141] The CFTC views Bitcoin and other virtual currencies as

payments, they are a key source" of suspicious transaction reports "on illicit financial flows related to ransomware.").

[139] *See* AMLBot, *Crypto Regulations in the US 2025: Complete AML & Compliance Guide* (Nov. 17, 2025), https://blog.amlbot.com/crypto-regulations-in-the-us-2025-complete-aml-compliance-guide/?utm_source= [https://perma.cc/SMP3-MHC7].

[140] *See* TRM Labs, *Sanctions screening* (last visited Apr. 3, 2026), https://www.trmlabs.com/glossary/sanctions-screening#what-is-sanctions-screening-1 [https://perma.cc/28TX-TGJX].

[141] *See* SEC, *SEC Clarifies the Application of Federal Securities Laws to Crypto Assets* (updated Mar. 17, 2026), https://www.sec.gov/newsroom/press-releases/2026-30-sec-clarifies-application-federal-securities-laws-crypto-assets?utm_source [https://perma.cc/K8KY-ZD4A]; GovFacts, *Bitcoin and Cryptocurrency Regulation*

"commodities" under the Commodity Exchange Act, allowing it to police derivatives markets and pursue fraud and manipulation in spot markets.[142] This patchwork structure has produced what commentators describe as "regulation by enforcement," where legal obligations are often clarified through agency actions and litigation rather than proactive rulemaking.[143]

Despite the breadth of agencies involved in regulating cryptocurrency exchanges, none of these frameworks meaningfully address the central problem posed by non-custodial (unhosted) wallets explained in Part I. Because these wallets are controlled directly by users rather than intermediaries, they fall outside the BSA's definition of a "money services business," leaving FinCEN without a hook to impose KYC or reporting obligations.[144] Even OFAC's sanctions authority, while technically applicable to any U.S. person, operates only through intermediaries capable of blocking transactions

in the United States (last updated Dec. 6, 2025), https://govfacts.org/money/investing-retirement/cryptocurrency-digital-assets/bitcoin-and-cryptocurrency-regulation-in-the-united-states/ [https://perma.cc/M5HZ-P2PU].

[142] GovFacts, *supra*, note 141.

[143] *Id.*

[144] *See* U.S. Dep't of the Treasury, *The Financial Crimes Enforcement Network Proposes Rule Aimed at Closing Anti-Money Laundering Regulatory Gaps for Certain Convertible Virtual Currency and Digital Asset Transactions* (Dec. 18, 2020), https://home.treasury.gov/news/press-releases/sm1216?utm [https://perma.cc/9ZFR-MGMG] (describing unregulated, unhosted wallets as "loopholes that malign actors may exploit."). FinCEN proposed extending reporting requirements to unhosted-wallet transactions in 2020, but withdrew the proposal in 2024 amid industry dissatisfaction. *See* Ethan G. Ostroff, *FinCEN Officially Withdraws Know-Your-Customer Rule for Non-Custodial Crypto Wallets*, TROUTMAN PEPPER LOCKE (Sept. 26, 2024),249 https://www.consumerfinancialserviceslawmonitor.com/2024/09/fincen-officially-withdraws-know-your-customer-rule-for-non-custodial-crypto-wallets/#:~:text=and%20litigation%20issues-,FinCEN%20Officially%20Withdraws%20Know%2DYour%2DCustomer%20Rule,for%20Non%2DCustodial%20Crypto%20Wallets&text=On%20August%2019%2C%20the%20U.S.,on%20non%2Dcustodial%20cryptocurrency%20wallets.

– an enforcement model that breaks down when no intermediary exists. Securities and commodities regulators likewise reach only the platforms that facilitate trading, not the private-key software individuals use to store assets. This regulatory blind spot enables ransomware actors and other illicit actors to move funds through unhosted wallets with little friction or visibility.

C. *Legislative Developments*

Despite the current agency-led nature of cryptocurrency exchange regulation, there is bipartisan support for more effective digital asset regulation in Congress. Most notably, the Guiding and Establishing National Innovation for U.S. Stablecoins ("GENIUS") Act was signed into law in July 2025, marking the first major federal law governing cryptocurrency. The GENIUS Act aims to incentivize competition and expand the digital currency market by regulating a specific type of digital asset called stablecoins.[145] Stablecoin currencies, which make up a large portion of all crypto transactions,[146] differ from traditional forms of cryptocurrency because they are backed by another form of real currency, like the U.S. dollar – a model designed to maintain stability of the currency's market.[147] While the perceived price stability of stablecoins stimulates legitimate crypto transactions, the same quality has made the currency "the preferred asset for terrorist financing and other forms of illicit activity[.]"[148] Fortunately,

---

[145] Max Zahn, *What to know about the GENIUS Act, a crypto regulation bill*, ABC NEWS (June 18, 2025, 10:44 AM), https://abcnews.go.com/Business/genius-act-crypto-regulation-bill/story?id=121981442.

[146] TRM Labs, *GENIUS Act Passes Senate, Paving the Way for Landmark US Crypto Legislation* (June 17, 2025), https://www.trmlabs.com/resources/blog/genius-act-passes-senate-paving-the-way-for-landmark-us-crypto-legislation#:~:text=Licit%20vs.%20TRM's%20analysis%20of%202024%20transaction,finance%20(DeFi)%2C%20digital%20commerce%2C%20and%20cross%2Dborder%20remittances (estimating that more than 60% of crypto transactions use stablecoins).

[147] *Id.*

[148] *Id.*

the GENIUS Act will subject stablecoin issuers to the BSA's AML and anti-terrorism financing requirements.[149] However, exchanges remain regulated only insofar as they list assets that fall within an existing agency's statutory remit. Aside from the requirement that an issuer retain procedures for freezing coins involved in illicit activity (regardless of whether those tokens are stored in a custodial or non-custodial wallet), unhosted wallets continue to fall outside all federal licensing, KYC, or reporting frameworks.[150] Though the GENIUS Act does not account for the unhosted wallet problem, it at least signals greater momentum towards disincentivizing illicit crypto transactions.

VI. Considerations for Covered Entities in the Healthcare Sector

While hospitals considered covered entities under CIRCIA may disagree with the suggested Cyber Emergency Alert system given the negative publicity or costs it may entail, their position will likely remain the same, or even benefit, from a ransomware attack public notification system.

In addition to the protections provided by CIRCIA itself, public disclosure of ransomware attacks may provide an extra layer of liability protection for a hospital's response, or non-response, to a ransomware attack. It should first be noted that, under the proposed rules, a covered entity would not be subject to lawsuits by virtue of submitting a report pursuant to CIRCIA's requirements. CIRCIA

[149] *See* Nellie Liang & William C. Dudley, *Next steps for GENIUS payment stablecoins*, Brookings (Mar. 6, 2026), https://www.brookings.edu/articles/next-steps-for-genius-payment-stablecoins/.

[150] *See* Evan T. Abrams et al., *The GENIUS Act and Financial Crimes Compliance: A Detailed Guide*, Steptoe (Aug. 22, 2025), https://www.steptoe.com/en/news-publications/blockchain-blog/the-genius-act-and-financial-crimes-compliance-a-detailed-guide.html#:~:text=Such%20secondary%20freezing%20would%20include,create%20complexities%20in%20certain%20contexts.

itself provides covered entities with liability protection for "litigation that is solely based on the submission of a covered cyber incident report" and prohibits such reports from being received in evidence or subject to discovery.[151] Moreover, any report submitted under CIRCIA is anonymized before disclosure to non-federal entities and exempt from disclosure under the Freedom of Information Act ("FOIA").[152]

On top of these protections, effectively compelling public disclosure of ransomware attacks may further insulate hospitals from liability relating to the kinds of claims based on fraudulent non-disclosures, like those made by Ms. Kidd. As an initial matter, if she had received a Cyber Emergency Alert about the ransomware attack, Ms. Kidd would not have even been admitted to the hospital in the first place because she would have presumably chosen a different hospital altogether. And even if Ms. Kidd did present to the hospital despite notice of the attack, the truth of the danger potentially resulting from receiving care there would have been fully disclosed to a geographically large range of people, so the attacked hospital would be remiss to represent otherwise.

While the more intangible cost of bad publicity may be very real for a hospital if the government were to publicly disclose that it has been hit by a ransomware attack, that cost may be substantially lower than that required to defend or settle consequent lawsuits in the absence of disclosure. This is likely especially true when the damage occurs to people, not just data, as in the *Kidd* case. From an optics perspective, more bad publicity may – and arguably should – derive from a hospital's failure to remediate the effects of a ransomware attack than its affirmative, public notification of such an attack. In the former scenario, the institution charged with saving lives appears to let its patients suffer, even die, in order to save face. In the latter

[151] 6 U.S.C. §§ 681e (c)(2)-(3).
[152] 6 U.S.C. §§681e(b)(2), 681e(d).

scenario, at least patients can trust the hospital to prioritize its patients' lives over business continuity and profits.

Moreover, applying the Cyber Emergency Alert framework to the healthcare sector seems particularly appropriate considering that hospitals are already held to similar data breach reporting requirements under the HIPAA Breach Notification Rule, as explained in Part II. If breach of protected health information warrants notification to both affected individuals *and the media* under the HIPAA Rule, the potential danger of bodily harm from a ransomware attack demands at least a proportional response.

VII. REMAINING CHALLENGES

While the suggested Cyber Emergency Alert system combined with CIRCIA's reporting requirements would signify a major improvement in public safety outcomes, there are still remaining challenges to mitigating the ransomware attack threat.

A lingering problem is the perpetuation of healthcare entities paying ransom demands and therefore the perpetuation of ransomware attacks themselves. While the U.S. government "strongly discourages" making ransom payments,[153] they are currently only illegal if made to sanctioned entities. Neither CIRCIA nor the suggested Cyber Emergency Alert approach create additional legal ramifications for paying a ransom demand.

There are a multitude of arguments for and against a complete ban on all ransom payments, and stakeholders are sharply divided on this issue. Proponents of a ban argue that prohibiting ransom payments will break the cycle of ransomware attacks primarily by

[153] U.S. Dep't of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* at 1 (Sept. 21, 2021), https://ofac.treasury.gov/media/912981/download?inline [https://perma.cc/6R7K-WF46].

"depriv[ing] the ransomware ecosystem of fuel."[154] As the FBI notes, "[p]aying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities."[155] Banning payments altogether could eliminate pressure to acquiesce to a ransom demand and incentivize victims to invest in cybersecurity or "bear the full costs of the damage their negligence induces."[156] Opponents of a ban assert that prohibiting ransom payments could backfire by incentivizing perpetrators to target entities most likely to pay a ransom demand, like hospitals, which only increases a perpetrator's likelihood of success.[157] FBI Cyber Division officials have added that banning ransom payments would only dissuade victims from reporting ransomware attacks to the government and potentially result in double extortion.[158] Further, some argue that a ban could entice victims to "hack back," which could render the victim susceptible to criminal charges under the Computer Fraud and Abuse Act ("CFAA").[159] Ban or not, without a major change in incentive structures, hospitals are especially likely to continue paying ransom demands given the lives, sensitive data, and reputational considerations at stake.

Further, geographic disparities and emergency medical situations may threaten a patient's ability to seek services from alternate healthcare facilities when faced with news of a ransomware attack at their original, chosen facility. This concern is especially

[154] Marañon & Wittes, *supra* note 134.

[155] *2023 FBI Internet Crime Report*, *supra* note 49, at 14.

[156] Marañon & Wittes, *supra* note 134.

[157] *Id.*

[158] Maggie Miller, *Top FBI official advises Congress against banning ransomware payments*, THE HILL (July 27, 2021), https://thehill.com/policy/cybersecurity/565110-top-fbi-official-advises-congress-against-banning-ransomware-payments/.

[159] Nicholas Winstead, *Hack-Back: Toward A Legal Framework for Cyber Self-Defense*, AM.U. CENTER FOR SEC., INNOVATION, AND NEW TECH. (June 26, 2020), https://www.american.edu/sis/centers/security-technology/hack-back-toward-a-legal-framework-for-cyber-self-defense.cfm.

prominent in rural areas where hospitals may be sparsely located and limited by staffing shortages or mechanisms for diverting patients to more sophisticated facilities.[160] It's not clear that these surrounding facilities would have the physical capacity or medical expertise needed to compensate for the victimized hospital's unavailability. However, the Cyber Emergency Alert system would at least put these surrounding health organizations on notice of the attack, as explained in Part IV.

Lastly, while beyond the scope of this writing, cyber incident insurance likely worsens the ransomware attack epidemic against the healthcare sector. Affected hospitals often rely on insurance to compensate for the damage caused by a ransomware attack rather than prevent the attack in the first place. Given that many policies actually *cover ransom payments*[161] and anecdotal evidence suggesting that some cyber attackers specifically target entities with cyber insurance,[162] its unsurprising that ransomware is "the single largest driver of cyber insurance claims."[163] This incentive structure arguably leads to healthcare entities taking a reactive, rather than proactive, approach to cybersecurity – one of the central phenomena underlying

[160] *See* Hannah T. Neprash et al., *Understanding the Rise of Ransomware Attacks on Rural Hospitals*, UNIV. OF MINN. RURAL HEALTH RSCH. CTR. (June 2024), https://rhrc.umn.edu/wp-content/uploads/2025/04/Understanding-the-Rise-of-Ransomware-Attacks-on-Rural-Hospitals-2024April-2025-Revised.pdf [https://perma.cc/86VG-JTNA].

[161] *See* Kyle D. Logue & Adam B. Shniderman, *The Case for Banning (And Mandating) Ransomware Insurance*, 28(1) CONN. INS. L.J. 247 (June 2022) ("[R]ansom payments are increasingly being covered by insurance."); *see* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks [https://perma.cc/7QYB-XKBR].

[162] *See Ransomware Task Force*, *supra* note 133, at 13.

[163] McMahon, *supra* note 8, at 195; *Ransomware Task Force*, *supra* note 133, at 13 ("Ransomware attacks are the most common reported cyber insurance claim").

the healthcare sector's disproportionate vulnerability to ransomware attacks.[164]

CONCLUSION

Ransomware attacks against U.S. critical infrastructure, especially those within the healthcare sector, pose a significant threat to both national security and public safety. While CIRCIA will serve as an important mechanism for informing the government's response to ransomware attacks, public notification of ransomware attacks against healthcare entities is necessary to mitigate consequent physical harm and deter national security threats. Issuing a new rule modeled after the HIPAA Breach Notification Rule will better protect hospital patients from the threat of bodily harm posed by ransomware attacks. This new provision can be administered by providing Cyber Emergency Alerts to the public through FEMA's established public safety alert system, IPAWS, or a successor system. This approach is unlikely to overburden American hospitals given CIRCIA's substantial liability protections and the requirements already imposed by HIPAA on most healthcare entities. CISA's JRTF should, in line with its statutory purpose and in coordination with the FBI and FCC, explore the viability of the proposed Cyber Emergency Alert system.

Further, the critical role of cryptocurrency exchanges in the facilitation of ransom payments deserves greater consideration when it comes to preventing and deterring ransomware attacks against critical infrastructure. Compliance with CIRCIA's ransom payment reporting requirements will assist CISA and other federal agencies in "following the money" to more effectively locate crypto wallets used to receive ransom demands and assign responsibility for ransomware attacks. Moreover, while the current state of federal crypto regulation is largely underdeveloped, Congress' focus on creating a federal regulatory framework is a promising path to a more robust digital

[164] *See supra* Part I.

asset ecosystem, as long as it prioritizes measures to deter illicit crypto-enabled activities.