Saint Louis University Journal of Health Law & Policy

Volume 11
Issue 2 *Supply Side and Demand Side Approaches to Health Care Financing*

Article 7

2018

Finding an Unlikely Combatant in the War Against Ransomware: Opportunities for Providers to Utilize Off-Site Data Backup Within the HIPAA Omnibus and Hitech Amendments

Jordan Butler
Jordan.Butler@slu.edu

FINDING AN UNLIKELY COMBATANT IN THE WAR AGAINST RANSOMWARE: OPPORTUNITIES FOR PROVIDERS TO UTILIZE OFF-SITE DATA BACKUP WITHIN THE HIPAA OMNIBUS AND HITECH AMENDMENTS

ABSTRACT

Each day the health care sector is subjected to an onslaught of thousands of ransomware virus attacks which attempt to capture a provider's IT operations until a ransom is paid to the hacker. Apart from monetary, functional, and civil liability considerations, compromised health systems that contain electronic patient health information could expose a provider to legal liability under multiple HIPAA laws. This article will explore how recent amendments made to HIPAA, particularly under the Omnibus and HITECH Acts, incentivize providers to obtain legal, functional, and policy-based benefits by utilizing off-site data backup business associates as part of their cybersecurity defense strategy in the escalating war against ransomware.

I. INTRODUCTION

In the age of big data where electronically protected health information (ePHI) is dominating the health care industry, "ransomware" attacks are increasingly becoming an issue for health care providers.[1] Ransomware is a form of malware, which takes the infected system and either blocks software usage on a computer, encrypts the computer's data, or both.[2] If the owner of the infected system does not pay a ransom, then she will not regain access to her computer and all files may be lost or, even worse, taken by hackers. These attacks have been occurring almost 4,000 times daily in the health care sector since the beginning of 2016.[3]

The frequency of ransomware attacks is increasing. For providers specifically, data systems held ransom for just a few minutes could lead to enormous monetary losses in both a functional and legal sense. When an attack encrypts a provider's data, there is a loss of functionality in how the provider makes money, a reputational hit, and numerous civil and government lawsuits coming from incidents that occur while the systems are down, such as losing ePHI. Perhaps the biggest consequence facing providers are the Health Insurance Portability and Accountability Act (HIPAA) civil monetary sanctions flowing from the 2009 HIPAA amendments.[4] The civil monetary cap per HIPAA violation is now $1.5 million.[5] Additionally, providers that are not properly prepared incur a financial cost by paying the ransom. In some cases, providers have already done so, finding it was in their best interest to resume business functions and pay the hacker's fee.[6] Given these serious ramifications, it is critical that health care entities dealing in ePHI develop strategies to protect their legal liability before, during, and after a ransomware attack. Accordingly, Congress has provided amendments to HIPAA, which providers should carefully consider when constructing their cybersecurity strategy. Particularly, four points from the Omnibus and Health Information Technology for Economic and Clinical Health (HITECH) Act amendments are crucial to ransomware considerations: (1) The maximum annual cap for civil monetary penalties

1. Kacy Zurkus, *The Rise of Ransomware in Healthcare*, CSO (July 11, 2016), http://www.csoonline.com/article/3091080/security/the-rise-of-ransomware-in-healthcare.html (last visited Feb. 20, 2018).

2. KEVIN SAVAGE ET AL., SECURITY RESPONSE: THE EVOLUTION OF RANSOMWARE 6 (2015), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.

3. DEP'T OF HEALTH & HUMAN SERVS., *FACT SHEET: Ransomware and HIPAA* 1 (2015), https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

4. Jessica J. Wilkes, Comment, *The Creation of HIPAA Culture: Prioritizing Privacy Paranoia Over Patient Care*, 2014 BYU L. REV. 1213, 1227 (2014); 45 C.F.R. § 160.404 (2013).

5. Wilkes, *supra* note 4, at 1228; 45 C.F.R. § 160.404.

6. Brittany Meiling, *A New Health Threat*: *Ransomware Attacks Target Hospitals, Holding Critical Patient Data Hostage*, SAN DIEGO BUS. J., Jun. 6, 2016, at 16.

(CMPs) has increased to five million dollars;[7] (2) business associates are now directly liable to the Department of Health and Human Services (HHS) for HIPAA violations;[8] (3) the definition of business associates has expanded to encompass any "subcontractor that creates, receives, maintains, or transmits protected health information";[9] and (4) assessment of the proper CMP charged against the provider has changed to a newly formulated tier structure dependent on culpability and expediency in curing the violation.[10]

This paper will argue that in response to the HIPAA Omnibus and HITECH amendments, health care providers should subcontract off-site data backup business associates to obtain legal, practical, and policy-based advantages in the ongoing battle against ransomware. As a primer, I will explain ransomware, its prevalence in health care, why it has become so ubiquitous generally, and the best practices applied to combat the cyberattacks thus far. Many providers have enacted incident response procedures, staff training, and other preventative practices such as anti-malware programs.[11] However, most of these strategies serve little use once a hacker has instigated an attack. In the third section, I will explore the 2013 HIPAA Omnibus amendments as well as the HITECH amendments, specifically focusing on their language towards business associates and liability. Before the Omnibus changes, almost all legal responsibility went to the provider regardless of their business associates' activities. With new amendments, there are incentives to outsource highly technological procedures to those who can perform them best and do so without increasing exposure to the provider itself. I will argue under the Omnibus Amendments a significant share of legal liability will pass to a third-party business associate in the event of a ransomware breach while concurrently reducing the sanction placed on the health care provider.

The fourth and fifth sections of this paper will explain off-site data backup as well as the legal, practical, and policy-based benefits that follow. Legally, I will explore how shifts in CMPs and certain definitional changes have incentivized using off-site data backup providers. I will also explore the practical advantages from the practice of having an off-site backup, including providing the highest quality care, minimizing administrative burdens, and continuing revenue-generating operations. This method essentially allows the provider to

7. 45 C.F.R. § 160.404; Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 1320d-5 (2016).

8. 45 C.F.R. § 160.402.

9. *Id.* § 160.103.

10. *Id.* § 160.408.

11. Jennifer L. Rathburn & Jennifer J. Hennessy, *Top Ten Health Law Issues of 2016: Cybersecurity*, AM. HEALTH LAWS. ASS'N CONNECTIONS, Feb. 2016, at 14; MURUGIAH SOUPPAYA & KAREN SCARFONE, U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBL'N 800-83 REVISION 1, GUIDE TO MALWARE INCIDENT PREVENTION AND HANDLING FOR DESKTOPS AND LAPTOPS ix (2013).

resume functions where it left before the attack, to do so without paying the ransom, and to abandon the hacker with encrypted data. Here, I will use a comparative study of an attack on Hollywood Presbyterian Medical Center and a separate attack on Alvarado Hospital Medical Center to demonstrate the benefits of having a robust off-site data backup system in place and how it is best to leave the technological jobs to the industries most knowledgeable about the subject. Finally, I will explore the policy-based advantages of using off-site business associates, such as removing incentives for ransomware attackers and protecting patient confidence in the ability of health care providers, to protect sensitive information.

The final section concludes that the HIPAA Omnibus and HITECH amendments have allowed an opportunity for hospitals to combat a technological threat occurring daily and the legal, practical, and policy-based advantages gained from using an off-site data backup are far too profitable to ignore.

II. BACKGROUND: RANSOMWARE IN HEALTH CARE

The first step to developing a strategy against ransomware is to understand what it is. Ransomware has been identified by HHS as a virus intended to damage or disable computer systems with the distinct characteristic of attempting to block the system's user from accessing data.[12] It is important to note that there are two forms of ransomware in circulation today. The most common type is called crypto-ransomware which blocks access to files by encrypting the system's data.[13] In theory, if the provider pays the ransom, then the hacker decrypts the data instantly, but in reality, the hacker could just demand more money. The second type of ransomware is called locker ransomware, which locks down the operating system or particular computer programs so that the user may not access the data inside those programs.[14] This paper will focus solely on crypto-ransomware.

A detailed understanding of the intricacies of crypto-ransomware are unnecessary to combat the virus, but every provider should have a basic knowledge of the anatomy of such an attack. Crypto-ransomware begins with an initial infection of some technological device linked to the provider's network.[15] The ransomware installs itself on the device and establishes permissions to start automatically every time the computer boots up.[16] Once attached to the device, the ransomware sends a message to the hacker who is responsible for the

12. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 3, at 1.
13. SAVAGE ET AL., *supra* note 2, at 3.
14. *Id.*
15. Meiling, *supra* note 6, at 16.
16. *Id.*

attack.[17] A technological "handshake" occurs between the hacker and the ransomware, creating an encrypted key that is stored on the hacker's server.[18] Once the hacker has the key, the ransomware begins encrypting all the files it can find.[19] After the hacker has control of the provider's records, the hacker demands a ransom in return for the key that unlocks the files.[20]

Surprisingly, ransomware has existed since 1989.[21] It is only recently that users of the malware have turned their attention toward medical data. This data has become more susceptible to attacks because protected health information has become a currency on the black market, possessing far more value than a credit card number or other personally identifying information.[22] An individual's medical records contain vast intelligence on their personal life including a social security number, previous and current addresses, names of siblings and children, and job history.[23] This type of record contains much more information and is much more valuable than a basic number generated from a credit card hack.[24] As such, Medicare or Medicaid records have been selling for $500 a-piece, which some experts estimate could be up to ten times the worth of a credit card number on the black market.[25]

The ransomware plague has infected the health care sector because of the value of protected health information. HHS reports a 300% increase from attacks in 2015 alone.[26] A separate report by Raytheon/Websense indicates that health care providers are 4.5 times more likely to face a crypto-ransomware attack than other industries.[27] Facing daily ransomware threats and severe CMPs, health care providers have developed some general practices that help, but by no means eradicate, the crisis.[28] For starters, it is commonly advised that providers protect their systems with some form of anti-malware.[29] While this is a necessary

17. *Id.*

18. *Id.*

19. *Id*.

20. Meiling, *supra* note 6, at 16.

21. Zurkus, *supra* note 1, at 3; Nsikan Akpan, *Has Health Care Hacking Become an Epidemic?*, PBS: NEWS HOUR (Mar. 23, 2016, 6:19 PM), http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic/ (last visited Feb. 20, 2018).

22. RAYTEHON & WEBSENSE, 2015 INDUSTRY DRILL-DOWN REPORT: HEALTHCARE 4 (2015), https://www.websense.com/assets/reports/report-2015-industry-drill-down-healthcare-en.pdf; Akpan, *supra* note 21.

23. Akpan, *supra* note 21.

24. *Id.*

25. *Id.*

26. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 3, at 1 (*citing* U.S. DEP'T OF JUSTICE ET AL., HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 2 (2016), https://www.justice.gov/criminal-ccips/file/872771/download).

27. RAYTEHON & WEBANESE, *supra* note 22, at 9.

28. *See id.* at 7.

29. *See* Meiling, *supra* note 6, at 16.

precaution, studies of ransomware attacks show that hackers may enter through periphery devices that do not have malware protection, such as cell phones.[30] Another practice implemented by health care providers is to encrypt patient data.[31] While also helpful, this practice serves little use in a crypto-ransomware attack, where a hacker has, in fact, encoded the provider's already-encrypted data. Thus, the encryption method blocks the hacker from accessing the data initially, but it does not help the user gain access to data held for ransom.[32] Another consideration regarding hospital encryption is its effectiveness at preventing the hacker from gaining access to ePHI and thereby undermining the value of those records for resale on the black market. Experts maintain unencrypted data has been a huge reason behind the majority of health care breaches partially because it is more difficult for hackers to retrieve and resell valuable patient information on the black market.[33] Assumedly, hackers may continue ransomware operations under the theory a provider will pay the ransom to get its records back. However, being able to prevent a profitable black market transaction of ePHI demonstrates the value of hospital encryption. While encryption is necessary for a hospital's defense strategy, it is not enough by itself to completely deter a hacker. Additional preventative practices such as off-site data backup are required. Other strategies recommended by HHS are conducting risk analysis assessments and training hospital staff to detect and report probable ransomware attacks to the proper people.[34]

Another suggested practice that health care providers were reluctant to latch on to because of the potential liability connected to a third party not controlled by the provider was having a reliable backup system of all the patient data with an off-site contractor.[35] In this situation, a third party maintains regular data backups of a provider's ePHI at an off-site server that, in theory, separates a copy of the ePHI from the crypto-ransomware infection.[36] Some reports in the early years of contracted business associates showed they were getting hacked more frequently than the actual providers themselves.[37] Moreover, before the Omnibus law, the health care provider incurred all legal liability for a breach of ePHI even if it occurred at a business associate's off-site location.[38] With exponential advances in information technology, data backup providers and

30. *Id.*

31. *See, e.g.*, DEP'T OF HEALTH & HUMAN SERVS., *supra* note 3, at 7.

32. *See* SAVAGE ET AL., *supra* note 2, at 5.

33. *See, e.g.*, RAYTHEON & WEBANESE, *supra* note 22, at 4.

34. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 3, at 1–2.

35. *See* Wilkes, *supra* note 4, at 1215.

36. *See, e.g.*, Joyce L. T. Chang, *The Dark Cloud of Convenience: How the HIPAA Omnibus Rules Fail to Protect Electronic Personal Health Information*, 34 LOY. L.A. ENT. L. REV. 119, 135 (2013).

37. Wilkes, s*upra* note 4, at 1231–32.

38. *Id*. at 1231.

other information technology business associates have become better at protecting ePHI.[39] This is likely because business associates are now directly liable to HHS for incredibly high CMPs in case of a breach, which give data protection vendors an additional incentive to provide the strongest protection possible.[40] No single practice for fighting against ransomware is dispositive, but rather a collection of methods that fit the provider's personal risk-benefit analysis should be implemented to fight the daily technology battle of protecting patient data. After the Omnibus and HITECH amendments, using an off-site data backup business associate to protect ePHI should be the foundation of every health care provider's collection of practices to defend against ransomware.[41]

III. OMNIBUS HIPAA LAW AND HITECH AMENDMENTS

On January 25, 2013, Congress enacted several changes to the HIPAA Omnibus law. Three of these changes significantly altered the way health care providers develop their internal policies to fight ransomware.[42] First, the new rules substantially raised the CMPs placed on health care organizations for patient privacy violations including ransomware breaches.[43] It also made business associates directly liable to HHS for their violations.[44] Congress also made numerous definitional changes by expanding who is accountable for HIPAA violations and what constitutes a breach of ePHI. The term "business associate" now encompasses third parties with whom hospitals, working with ePHI, contract.[45] The definition of "breach" has also expanded to encompass even a risk of ePHI disclosure or improper use of such information as determined through a risk assessment analysis.[46] This is a significant change from the previous definition of breach, which was any event that "compromises the security or privacy of the protected health information such that the use or

39. Dan Turkel, *Even the Best Antivirus Likely Can't Save Your Files from a Ransomware Infection*, BUS. INSIDER (Jan. 24, 2016), http://www.businessinsider.com/fighting-ransomware-with-antivirus-2016-1 (last visited Feb. 20, 2018).

40. Wilkes, s*upra* note 4, at 1229.

41. Ann Killilea & Michael G. Morgan, *Guidance on Ransomware Attacks under HIPAA and State Data Breach Notification Laws*, MCDERMOTT WILL & EMERY (Aug. 8, 2016), http://1npdf9.cloudapp.net/pdfrenderer.svc/v1/ABCpdf9/GetRenderedPdfByUrl//HIPAA%20Randsomeware%20Attacks%20State%20Data%20Breach.pdf/?url=https%3a%2f%2fwww.mwe.com%2fen%2fthought-leadership%2fpublications%2f2016%2f08%2fhipaa-randsomeware-attacks-state-data-breach%3fpdf%3d1&attachment=false.pdf.

42. Kevin Twidwell & Brianne McClafferty, *New HIPAA Rules Go into Effect: Lawyers Need to up Their Game in Protecting Private Health Care Information*, MONT. LAW., Dec.–Jan. 2013, at 14; Wilkes, s*upra* note 4, at 1229–30.

43. 78 Fed. Reg. 5566, 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164).

44. *Id.*

45. *Id.* at 5566–67.

46. *Id*. at 5640.

disclosure poses a significant risk of financial, reputational or other harm to the individual."[47] These definitional changes concerning who is liable and what triggers liability incentivize providers to create even more detailed cybersecurity plans and to share the risk of CMPs among business associates.

The financial changes for HIPAA sanctions also act as a significant incentive for health care organizations to avoid violations. The new cap for CMPs committed by a provider either knowingly or neglectfully is set at $1.5 million.[48] A health care provider can quickly reach the cap, considering that every unauthorized disclosure of ePHI may constitute not just one but many violations.[49] Because of this possibility, HHS has to assess the penalty amount based upon both the nature and the extent of the offense.[50] Crypto-ransomware attacks can easily compromise entire databases of ePHI.[51] It is therefore easy to see why providers increasingly worry about fines aggregating uncontrollably in the absence of a robust cybersecurity plan.

After the Omnibus amendments, business associates including data services are directly liable for breaches and HIPAA violations.[52] Thus, business associates, like providers, potentially face a $1.5 million CMP cap should they choose to contract with a provider.[53] Not only can the business associate experience monetary damages but also reputational harm. The infamous "Wall of Shame" at HHS publicly exposes any breach of protected health information which affects over 500 people.[54] For a data backup company whose revenue is derived almost exclusively from its ability to defend and store information, a national public reprimand highlighting its failure to successfully perform this task can lead to severe reputational harm. This amendment, therefore, incentivizes better security of ePHI, as it is in the associate's best interest to ensure compliance with HIPAA standards.

The expansion of direct liability for business associates additionally helps to address the issue of lacksadasical third-party security of ePHI. One biannual study of health care provider facilities suggests that business associates

47. *Id.* at 5639.

48. 78 Fed. Reg. at 5583.

49. *Id.* at 5584.

50. *HIPAA Violations & Enforcement*, AM. MED. ASS'N, https://www.ama-assn.org/practice-management/hipaa-violations-enforcement (last visited Feb. 11, 2018).

51. Loretta Duncan & Brian Johnson, *Ransomware Attacks, Brief Notifications, and Security Rule Compliance: What You Need to Know Now*, SVMIC SENTINEL 7 (Sept. 2016), https://www.svmic.com/Home/media/29938/sentinel-september-2016.pdf.

52. 78 Fed. Reg. at 5566.

53. *Id.*

54. Jessica Davis, *HHS Overhauls 'Wall of Shame' Breach Reporting Website*, HEALTHCARE IT NEWS (July 26, 2017, 11:29 AM), http://www.healthcareitnews.com/news/hhs-overhauls-wall-shame-breach-reporting-website (last visited Feb. 20, 2018).

previously constituted the most significant percentage of data breaches.[55] Furthermore, this study indicates a correlation between that portion of data breaches and the fact that those business associates were not held liable for their security measures.[56] Given this statistical framework, providers before the amendments were understandably reluctant to take on a contract with a business associate to backup ePHI. Not only was the provider liable for breaches caused by the business associate, but it was also responsible for conducting regular reviews and risk analysis assessments of the associate to ensure compliance.[57] This process resulted in a tremendous cost for the provider in oversight of the business associate with little to no reward regarding ePHI protection.[58]

Finally, another critical amendment is the tier structure for CMPs, created in the 2009 HITECH Act.[59] Mostly, penalties for violations of the HIPAA Security Rule vary based on the provider's culpability.[60] The changes distinguish fault into four categories.[61] To meet the lowest penalty level of "unknowing," the provider must not have known and reasonably should not have known of the impending incident.[62] The second tier, labeled "reasonable cause," applies to providers and business associates who knew or reasonably should have known but did not act with "willful neglect."[63] The highest two penalty category refers to entities which act with "willful neglect."[64] If the violation was the result of an entity's conscious disregard or reckless indifference on the matter, they will fall into one of these categories. Penalties of this type are lessened, however, for providers who correct the violation within thirty days of discovering what occurred.[65] This tiered structure incentivizes providers and business associates to develop stronger security policies to protect ePHI. The Secretary of HHS is also limited within the bill from enforcing CMPs against providers who do not act with willful neglect and correct the violation within

55. *See* Heather Landi, *Study: 30 Percent of Patient Data Breaches Involve Business Associates*, HEALTHCARE INFORMATICS (Sept. 21, 2016), https://www.healthcare-informatics.com/news-item/cybersecurity/study-30-percent-patient-data-breaches-involve-business-associates (last visited Feb. 20, 2018).

56. *See* KROLL ADVISORY SOLS., 2012 HIMSS ANALYTICS REPORT: SECURITY OF PATIENT DATA 6 (2012), https://csbweb01.uncw.edu/people/CummingsJ/classes/MIS534/Articles/Previous%20Articles/Ch6SecurityReport.pdf.

57. 45 C.F.R. § 164.302–08 (2013).

58. KROLL ADVISORY SOLS., *supra* note 56, at 28–35.

59. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 1320d-5 (2016).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. 42 U.S.C. § 17939.

65. *Id.*

thirty days.[66] This limitation demonstrates the incentive for a well thought out and responsive cybersecurity strategy on the part of providers.[67]

Four different amendments, three to the Omnibus HIPAA law and one to the HITECH Act, when considered together, create a sound policy incentive for providers to use business associate services to backup their data. An enormous expansion of liability to HHS for HIPAA compliance occurred with the addition of business associates.[68] Providers are now allowed to share responsibility and thus the overall cost of a breach with their subcontracted associates.[69] Security of a provider's ePHI will increase because now the backup services are directly liable themselves for ePHI violations. Therefore, providers have both monetary and reputational interest in the matter, which strengthens the overall effort toward data protection. Additionally, the definitional, liability, and CMP amendments concurrently allow a health care provider to minimize its responsibility and financial exposure while shifting a technological function to an entity far more qualified to handle the task of protecting ePHI.

IV. OFF-SITE DATA BACKUP PROVIDERS

One practice providers should consider adding to their bundle of cybersecurity methods is using off-site data backup so that, if a provider's on-site ePHI is hacked, the provider can retrieve or otherwise access the same ePHI from the off-site backup. In the event the off-site business associate is hacked, the HIPAA liability for the disclosure in that instance belongs to the third party.[70] Using business associates and particularly off-site data backup services, a health care provider's liability regarding the nature and extent of a breach to ePHI during a ransomware attack could be limited substantially by controlling how much access to ePHI the hacker ultimately achieves and how much bargaining power the hacker has over the hospital. By preventing an excessive breach using the data backup services, the health provider has certainly minimized the legal, practical, and policy-based consequences it would incur from the attack.

The use of contracted associates—such as data backups and cloud services to store electronic data—is an ongoing trend in health care as well as other

66. *Id.*

67. *Id.* § 17938.

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

69. *Id.*

70. *Id.* at 5639.

industries.[71] But not all providers maintain off-site data backups.[72] The lack of use of such measures could be due to lack of awareness of changes in liability exposure due to the Omnibus amendments, costs of using such a security provider, or a health care provider opting to follow an alternative storage method such as a paper system.[73] Regardless of the reason health care providers did not use a business associate before, the changes to the HIPAA Omnibus Rule and HITECH Act indeed indicate they should use one now for data backup. In regards to their services for health care providers, data backup providers furnish frequent backups of ePHI which is continually updated and stored at an off-site location.[74]

From the perspective of a hospital's functionality during a crypto-ransomware attack, having a backup of data is an enormous strategic advantage. As previously explained, a crypto attack encrypts the user's data making it unusable until the owner of the files pays a ransom.[75] However, if the provider has opted to use an off-site business associate, then it has a non-ransomware infected version of its records at the ready and can leave the hacker with the encryption key for the hacked files.[76] This action would be okay, assuming the provider was already implementing its encryption practices for the ePHI.[77] Thus, using this method, the provider would access its backup system, and even if the hacker removed his encryption from the initial attack, the hacker could not access the files because they still maintain their base security encryption placed on the data by the health care provider.

Beyond the functional advantages of using an off-site data backup system, there are huge monetary and reputational benefits for health care providers to consider. First, during a ransomware attack, a hospital will lose a significant percentage of its functionality if it cannot access its files.[78] Doctors are unable to see patients, operations cannot be performed, and even administrative functions are blocked because critical records are being held to ransom. By having an at-the-ready backup system in place, it is essentially like the attack

71. Anne DiNardo, *Healthcare Data Centers: Carrying the Load*, HEALTHCARE DESIGN (Aug. 25, 2014), http://www.healthcaredesignmagazine.com/trends/architecture/data-centers-carrying (last visited Feb. 2, 2018).

72. *See id.*

73. *Id.*; *see* 78 Fed. Reg. at 5566, 5575.

74. *See* EMC HEALTHCARE SOLS., TRUSTED IT SOLUTIONS FOR HEALTHCARE PROVIDERS: BEST PRACTICES FOR HEALTHCARE PRIVACY AND SECURITY REQUIREMENTS 5 (2014), https://www.emc.com/collateral/white-papers/h12709-trusted-it-solutions-healthcare-wp.pdf.; *see generally* SYMANTEC, SECURITY AND PRIVACY FOR HEALTHCARE PROVIDERS 10 (2009), http://eval.symantec.com/mktginfo/enterprise/white_papers/b-security_and_privacy_for_healthcare_WP_20934020.en-us.pdf.

75. *See* s*upra* discussion Part I.

76. Meiling, *supra* note 6, at 16.

77. *Id.*

78. Zurkus, *supra* note 1, at 1.

never happened. A hospital can resume its normal operations and lose little to no money as a result.[79] Moreover, the provider is able to protect its reputation related to providing quality, confidential health care and protecting patient data. As a result of the recent uprising in cyberattacks on the health care sector, patient trust has taken a significant hit because of consumers who feel providers are not taking adequate steps to safeguard their personal information.[80] A provider that shows it has thought carefully about and developed strong cybersecurity measures against hackers will preserve, and arguably gain more, reputational value and clients because of a demonstrated dedication to patient privacy.

A comparative study of two hospitals, one of which implemented the practice and one of which did not, demonstrates the practical advantages to be gained from using an off-site data backup service.[81] In early 2016, a crypto-ransomware attack known as "Locky" hit Hollywood Presbyterian Medical Center located in Los Angeles.[82] The attack crippled the hospital's functionality when it took computers offline for over a week.[83] Because Hollywood Presbyterian did not have off-site data backup, the hospital felt it only had one option, and the board eventually decided that it was in its practical and reputational best interest to pay the ransom of $17,000 in an untraceable currency known as Bitcoin.[84] Shortly after the Hollywood Presbyterian attack, another crypto-ransomware attack hit San Diego-based Alvaredo Hospital.[85] A representative for the hospital later claimed because of Alvaredo's robust off-site data backup, it did not have to pay the ransom or even negotiate with the hacker.[86] Instead, it was able to turn to its backup data, resume regular hospital functions, and terminate communications with the hacker. The hospital's spokesperson and several analysts agree it was the off-site data backup that saved Alvaredo hospital the day of the attack.[87]

Two critical observations emerge from this comparative study. First, the hospital that did not have any form of data backup fell prey to ransomware and was forced to pay a ransom to resume standard revenue-generating and life-saving hospital functions. Alternatively, Alvaredo Hospital maintained strong, consistent data backup and, as such, did not even need to negotiate with the

79. Meiling, *supra* note 6, at 16.

80. Asha Saxena, *6 Ways Hospitals Can Ease Patients' Fears About Security Threats*, BECKER'S HOSP. REV. (May 26, 2015), https://www.beckershospitalreview.com/healthcare-information-technology/6-ways-hospitals-can-ease-patients-fears-about-security-threats.html (last visited Feb. 20, 2017).

81. Meiling, *supra* note 6, at 16.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

86. Meiling, *supra* note 6, at 16.

87. *Id.*

hacker. Alvaredo had its defense procedures in place, and as a result, avoided functional and probable reputational losses similar to those Hollywood Presbyterian faced. Second, Alvaredo hospital did not just have data backup—it had off-site data backup. The off-site element is critical because ransomware may move through different interconnected networks within a single provider location encrypting the data as it goes along, including backups. Information technology scholars have suggested this is exactly what happened to Hollywood Presbyterian as the result of not having an off-site copy of their data they could revert to.[88] When comparing these recent events, the practicality of hospitals having a business associate that runs an off-site data backup center becomes apparent. Having such a backup ensures the hospital is ready for future ransomware attacks and that the hospital can continue to operate as planned providing safety to its patient's well-being, continuing revenue-generating functions, and protecting its reputation in the private sector as being able to protect ePHI safely.

V. THE LEGAL, FUNCTIONAL, AND POLICY-BASED ADVANTAGES AFTER THE AMENDMENTS

The benefits that flow from the use of business associates after the HIPAA Omnibus changes are numerous and will be discussed in terms of their legal, functional, and policy advantages, beginning with the practical legal advantages.

A. The Legal Advantages Stemming from Increased Penalties and Definitional Changes

The readjusted CMPs for ePHI violations present primary legal advantages to using off-site data backup associates. The annual financial cap for breaches of ePHI has increased to $1.5 million.[89] The increase per violation means providers should be more incentivized to develop policies that could implicate that penalty, including crypto-ransomware attacks. CMS considers the four-tier structure when assessing what level of penalty to apply.[90] Thus, a provider will be fined less in instances where it demonstrates the breach was the result of a reasonable cause rather than willful neglect of the issue.[91] Moreover, CMS significantly diminishes the penalties for providers who correct a violation caused by willful neglect within thirty days.[92]

88. *Id.*

89. Wilkes, *supra* note 4, at 1228.

90. *Id.*

91. Health Information Technology for Economic and Clinical Health (HITECH) Act, 42 U.S.C. § 1320d-5 (2016).

92. *Id.* Per HHS guidance, correction of a violation includes a "notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate." HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414; *see also Breach Notification Rule*, U.S.

Another set of legal advantages comes from additional definitional changes in the amendments, mainly that of what constitutes a "breach" of ePHI and the newly assigned shared legal liability for business associates. To review, violations of the Omnibus amendments have largely been expanded to cover any "risk" of ePHI disclosure.[93] Additionally, the Omnibus amendments expanded who was legally liable to HHS for such breaches.[94] Now, the business associates themselves are directly responsible for their violations.[95] These definitional changes mean providers and associates alike should take additional steps in developing their cybersecurity defense plans by working together through a shared liability framework.

When considering these various amendments, an off-site business associate can vastly minimize the cost for a provider in several ways. First, with newly tiered levels of penalties, the off-site contracted services would markedly demonstrate the provider has not exercised willful neglect of the issue of ransomware attacks.[96] Given the prevalence of ransomware attacks in the health care sector today, it would seem tough for a provider to argue they were not aware they could be a target for such a situation. Thus, the defensive action would help push a provider's penalty into the lower "reasonable cause" tier.

Second, the expansive definition of breaches implores providers to use off-site backup. Because hospitals and providers are now liable for even a "risk" of compromised ePHI, the best strategy is to nullify that risk by using an off-site business associate.[97] Crypto-ransomware spreads through the network of information at a facility's location, encrypting the data.[98] However, if the provider has previously encrypted its data, they have not reached the "risk" threshold in this phase of the cyberattack.[99] By having an off-site backup of the data, the provider leaves the hacker with double encrypted data: one base encryption by the hospital and one by the hacker.[100] The hospital can resume its functions without paying a ransom, similar to Alvaredo Hospital.[101] This added layer of protection ensures the provider will not have to work with the hacker to restore the hospital to standard functions, a factor which would undoubtedly weigh in on CMS' evaluation of whether there was a risk of compromised ePHI.

DEP'T OF HEALTH & HUMAN SERVS. (2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Mar. 26, 2018).

93. *See* 42 U.S.C. § 1320d-5.
94. *Id.*
95. *Id.*
96. *Id.*
97. 45 C.F.R. § 164.402(1)(ii) (2011).
98. Meiling, *supra* note 6, at 16.
99. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 3, at 7.
100. *Id.* at 7–8.
101. Meiling, *supra* note 6, at 16.

The next legal advantage to consider from subcontracting ePHI to an off-site business associate is shared liability between both providers and contracted business associates. Because business associates are now directly liable for breaches of ePHI, a provider who uses an off-site data backup service has significantly diminished the CMPs it would have otherwise paid for a business associate's violation. This liability sharing mechanism appears to be an effort by the legislature to aid the health sector by allowing coalition efforts with the technology industry to protect patient data. Because hospitals are overburdened with numerous health-related challenges, it makes sense for a provider to outsource such a highly technical task so that the provider can focus on the actual quality of care for its patients. The many benefits of this trend, and the simple principle of wanting to share liability rather than wholly assume it, demonstrates yet another reason providers should adopt the practice of contracting with an off-site data backup business associate.

Another legal benefit to consider is the number of private civil liability claims a hospital will avoid by being able to immediately resume function and patient care during a ransomware attack. By having an off-site data backup system in place, the hospital can continue its normal operating procedures and thus avoid potential harms to patients caused by downed technology systems. It is purely hypothetical to guess what could happen to patients inside of a hospital that suddenly loses its ability to treat, but the possibilities range from minor inconveniences such as scheduling confusion, to fatal outcomes. For a hospital to combat the systematic shutdown of its operations and avoid numerous civil lawsuits, it should have an off-site data backup system ready for when a crypto-ransomware attack strikes.

When considering the newly increased $1.5 million civil monetary penalty cap, the four-tiered penalty structure, and the expanded definitions regarding what constitutes a breach and who is liable for such a violation, the legal advantages to a provider contracted with an off-site data backup provider are evident. The contracting health care entity can diminish the likelihood it will ever even reach the cap by reducing the tier of possible penalty by developing and implementing a robust cybersecurity plan against ransomware attacks. Additionally, using off-site backup allows the provider to avoid negotiations with a hacker, and also consequently diminishes the likelihood of even a "risk" of compromising ePHI. Moreover, because of shared liability with the data backup provider, the provider may rest a little easier knowing it does not share the full pot of the penalties and that a job which calls for highly skilled technological knowledge is left to the sector best equipped to deal with such an issue. Finally, a provider can avoid harsh civil legal liability by being able to functionally maintain the level of care it provides to patients before a ransomware attack occurs.

B. The Functional Advantages Stemming from Being Able to Resume Revenue-Generating Operations

A health care provider may generate money in numerous ways, but a base point is undoubtedly its ability to attract, admit, and treat patients.[102] A crypto-ransomware attack cripples a provider's technology and thus can shut down the processes that generate revenue.[103] In some instances, these periods have lasted weeks and even longer for providers who refuse to pay the ransom.[104] The costs of a major hospital being shut down for hours are tremendous in and of themselves, and those costs multiply exponentially when systems are shut down for months or weeks. Another issue to consider is that even if the provider pays the ransom, it still does not know if the hacker will turn over the data as promised or just demand more money once he has found a willing negotiator. Having an off-site data backup business associate precludes the need to negotiate or consider paying the hacker's ransom demand.

By being able to quickly resort to an off-site data backup during a ransomware attack, the provider is advantaged functionally two-fold. First, it can continue to serve its ultimate purpose, which is to provide quality health care for those who need it. Without patient data, operating systems, and the ability to use medical technology in procedures, a hospital becomes more of a boarding location rather than a treatment facility for illnesses and diseases. Not only is the providence of medical services hindered but also the administrative duties of physicians and staff are profoundly burdened. One report from the AC Group indicates typical administrative responsibilities take physicians double the time to perform when systems are down.[105] This translates into additional cost considerations for the hospital's board when deciding whether or not to pay a ransom. The off-site backup allows physicians and medical staff to continue providing the highest level of care available because they are still working off the patient's known medical history and treating the patient with up-to-date medical technological devices. Additionally, it allows physicians to limit their time performing administrative duties which translates into more time for patient treatment and ultimately more revenue.[106]

The second functional advantage stems from the actual revenue flow of the provider itself. A hospital that can resume operations will not lose any revenue due to changes to its ability to care for patients that otherwise would have generated money for the hospital. It is the equivalent of any other business being

102. Patrick A. Rivers & Saundra H. Glover, *Health Care Competition, Strategic Mission, and Patient Satisfaction*: *Research Model and Propositions*, 22 J. HEALTH ORG. MGMT. 627, 629 (2008).

103. Meiling, *supra* note 6, at 15–16.

104. *Id.* at 16.

105. Zurkus, *supra* note 1, at 7.

106. Meiling, *supra* note 6, at 16.

completely shut down for a day. A company cannot make money if its doors are not open for the services it provides. A study by the Ponemon Institute estimates just one minute of downtime could cost a health care organization an average of $7,900.[107] The inability to make money from crippled data systems is likely why Hollywood Presbyterian Hospital decided to pay the nominal $17,000 its ransomware hacker was demanding after the hospital's operations were shut down for weeks.[108] This enormous price difference between what ransomware hackers are demanding and what the hospital may lose in revenue, unfortunately, incentivizes hospital boards to pay the ransom in order to protect the viability of the company. However, having an off-site data backup grants the provider a firmly rooted defensive strategy against such an attack, because functional revenue loss no longer exists as a consideration for negotiating with a hacker. Instead, the hospital resumes operations as if nothing ever happened.

Practically, it is also important to ask who is better equipped to deal with complicated ransomware software, the technology or medical sector. In addition to the daily demand on health care providers, developing top of the line cybersecurity systems can prove to be both a costly and timely endeavor.[109] Alternatively, business associates such as cloud and data backup providers have been focusing the bulk of their resources and attention on developing practices to combat ongoing cybersecurity threats.[110] Beyond the fundamental knowledge gap between the options of internally developing backup servers or outsourcing the activity, providers also must consider the cost of retaining all their electronic patient records in-house. Data servers are not cheap, and providers gain new patients every day while also having a duty to keep old records.[111] When considering maintaining a live backup of data, that provider must be aware it needs enough server space for two copies of an ever-growing collection of medical records.

There are also a number of practical factors to consider for health care providers assessing whether to establish their own data center or to outsource the function. First, the provider must evaluate how much size capacity they will require based on how many patients it treats. Additionally, the provider must consider how long certain cybersecurity options take to implement. For instance, a cloud storage option could be established much faster than off-site data

107. Zurkus, *supra* note 1, at 8.

108. Meiling, *supra* note 6, at 16.

109. DiNardo, *supra* note 71.

110. *How Safe is Online Backup?*, DATA BACKUP & ONLINE STORAGE, http://www.databackuponlinestorage.com/Online_Backup_Services_How_Safe (last visited Feb. 2, 2018); Sara Angeles, *Cloud vs. Data Center: What's the Difference?*, BUS. NEWS DAILY (Aug. 26, 2013, 5:49 AM), https://www.businessnewsdaily.com/4982-cloud-vs-data-center.html (last visited Feb. 20, 2018).

111. 45 C.F.R. § 164.530(j)(2) (2009); *see* ALA. ADMIN. CODE § 42-5-10-.03(33) (2011).

backups but may not provide the same degree of security for the ePHI.[112] Yet another consideration is where to place the data center. Some providers may elect to have on-site data storage while other will choose off-site options. Either option will require substantial use of real estate and could quite possibly require further construction and spending by the provider. Finally, a vital consideration for providers is whether or not to lease the data security services. Establishing such a contractual relationship would not only allow the provider to fall under the newliability laws regarding business associates, but also could turn the data center into an operational cost rather than a capital cost.[113] This is because the provider is not spending its own money to construct a data center but is rather investing in monthly payments.[114]

Amongst all these considerations there are also practical disadvantages for providers who establish their own live data centers. The most obvious is that if ransomware can affect the provider's primary data set of ePHI, it likely could reach its backup as well, and thus the advantage of having separate party data backup becomes apparent. The knowledge and infrastructural disadvantages a health provider faces in maintaining an internally developed and stored data backup system demonstrate the technological complexities providers face in protecting patient information. For instance, in 2015 alone, 362,000 new forms of ransomware were identified, averaging 1,000 new versions of the virus per day.[115] Not only is the health care industry facing the ransomware threat daily, but it is also likely facing a new form of the virus every time an attack is attempted. HHS gave health care providers a tool to tackle those technological disadvantages by encompassing subcontractors who work with ePHI as business associates of providers.[116] By subcontracting the specific technical work of ePHI backup to a dedicated expert entity, providers can focus on the functions of their knowledge and expertise, creating a stronger and more secure health care system for everyone.

The Omnibus and HITECH amendments grant health care providers enormous functional advantages when electing to contract with off-site data backup business associates. A hospital may continue to provide its highest level of care to patients from functionally being able to use the same systems and data in treatment. The hospital can also maintain revenue generation from being able to provide treatment for patients. Further, provider limitations on infrastructure

112. Angeles, *supra* note 110.

113. Ajmal Kohgadai, *Top 5 HIPAA-Compliant Cloud Storage Services*, SKYHIGH NETWORKS, https://www.skyhighnetworks.com/cloud-security-blog/top-5-hipaa-compliant-cloud-storage-services/ (last visited Feb. 2, 2018).

114. *Id.*

115. Brianna Gammons, *5 Things to Know About the Rise of Ransomware among Healthcare Providers*, BARKLY (June 2016), https://blog.barkly.com/rise-of-ransomware-healthcare-stats (last visited Feb. 21, 2018).

116. Kohgadai, *supra* note 113.

spending and possessing the requisite technical knowledge also encourage the use of off-site data vendors to protect ePHI.

C. The Policy-Based Advantages of Maintaining Patient Confidence in the Provider and Standing Up Against Ransomware Bullying

There are two significant policy benefits for health care providers to broadly contemplate when deciding whether to incorporate off-site data backup into its cybersecurity strategy. The first consideration is the overall confidence citizens have in the health care system and particular providers. The HIPAA security rule was created to protect patient health information in part because such information is sensitive and unique to every individual.[117] In order to be open to physicians and receive proper treatment, people should feel confident their private (and sometimes embarrassing) information is not exposed to those outside of the patient-doctor relationship or sold. If patients begin to believe that personally-identifiable, sensitive health information is at risk of exposure, people will be less candid when engaging with health care providers. In the aggregate, this effect could lead to fewer routine health checkups, higher rates of illnesses, and more costly courses of treatment to diagnose problems. Regarding particular hospitals, patients are less likely to choose a hospital for treatment if they know it has previously failed to protect patient health information.[118] This policy effect broadly leads to fewer patients seeking medical care, which is detrimental to both public health and the provider's revenue stream.[119]

With off-site data backups, providers can avoid the policy issue of patient confidence. Although resulting in a data backup and leaving the hacker with a key to encrypted information does not exactly recover the ePHI from the hacker's possession, it does demonstrate to the patients of that particular provider that protection of their sensitive information is a priority. Moreover, so long as the provider was providing baseline encryption for its ePHI, there likely would not be a breach of data, so the encrypted data is all the hacker can obtain.[120] By having an off-site backup defense strategy, the hospital projects

117. BARRY R. FURROW ET AL., HEALTH LAW: CASES, MATERIALS AND PROBLEMS 269 (7th ed. 2013).

118. Juhee Kwon & M. Eric Johnson, The Market Effect of Healthcare Security: Do Patients Care About Data Breaches? 3 (June 22, 2015) (unpublished manuscript), http://www.econinfosec org/archive/weis2015/program.html (last visited Feb. 21, 2018); FAIRWARNING, HOW PRIVACY CONSIDERATIONS DRIVE PATIENT DECISIONS AND IMPACT PATIENT CARE OUTCOMES 5 (2011), https://www.fairwarning.com/wp-content/uploads/2015/08/2011-09-WP-US-PATIENTSUR-VEY.pdf.

119. *Id.*

120. Jessica Davis, *Ransomware Rising, But Where Are All the Breach Reports?*, HEALTHCARE IT NEWS (Mar. 20, 2017), http://www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports (last visited Feb. 21, 2018).

confidence to its patients that it is well equipped to handle technological threats, allowing the patients to focus on getting treatment rather than where they can go for care without having their personal secrets revealed. Creating a robust cybersecurity defense that includes off-site data backups is, therefore, imperative for hospitals to maintain patient confidence in the course of health care treatment.

The second major policy consideration is creating disincentives for ransomware bullying by nullifying the possible monetary gains from such an attack. As discussed, ePHI has become heavily targeted by hackers because of its value on the black market due to the vast personal information each patient file contains.[121] Ransomware attackers have one objective: to hold precious information captive until some ransom is paid in exchange for its release. Additionally, hackers know the providers need ePHI to function normally and to treat patients. Therefore, to end this type of bullying, health care providers should seek to build cybersecurity frameworks that protect ePHI in a way in which hackers cannot leverage such information against them.

One of the simplest additions to a provider's existing cybersecurity structure would be to add an off-site data backup.[122] This would be a tremendously beneficial addition to a collection of protections designed to frustrate a hacker's ability to obtain ransom payments from a hospital or payments from the black market for stolen ePHI. For instance, by being able to resort to a carbon copy of the information taken, the provider no longer has reason to bargain for its retrieval. Instead, the provider can continue how it was operating as if the attack never occurred while also leaving the encrypted data with the hacker. Moreover, if the hospital included data encryption in its protection strategy, the hacker is equally unlikely to sell the ePHI on the black market. Not being able to quickly resort to data backup results in hospitals being non-operational for lengthy time periods, which then leads to needing to negotiate a ransom. This often forces providers to pay the hacker, which only affirms his and others' ability to make money off of such an act. It is in the interest of the health care sector overall to implement off-site data backups. Presumably, if hackers are continually unable to get any form of monetary compensation for their actions, they will stop the attacks or at least shift their focus towards another industry that is less prepared for such matters.[123]

121. Lucas Mearian, *Hackers Are Coming for Your Healthcare Records – Here's Why*, COMPUTERWORLD (June 30, 2016), https://www.computerworld.com/article/3090566/healthcare-it/hackers-are-coming-for-your-healthcare-records-heres-why.html (last visited Feb. 21, 2018).

122. Nate Lord, *Healthcare Cybersecurity: Tips for Securing Private Health Data*, DIG. GUARDIAN (July 26, 2017), https://digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data (last visited Feb. 6, 2018).

123. Robert Roohparvar, *5 Industries That Top the Hit List of Cyber Criminals in 2017* (July 18, 2017), http://www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (last visited Feb. 20, 2018); David Kidd, *Healthcare, Encryption and HIPAA Compliant Systems: How*

To protect patient confidence in the health care system and to put an end to ransomware bullying in the health industry, providers should utilize off-site data backup business associates. Doing so takes away the power of the hacker as the value of the encrypted ePHI he possesses is significantly diminished by the provider's ability to quickly revert to an up-to-date copy of the stolen data, and demonstrates to patients and the public how the provider is treating patient privacy as a top priority in the modern technological age.

VI. CONCLUSION

There is no doubt ransomware attacks are on the rise in the health care sector. The question is: what will the health care industry do to respond to the crisis? A robust cybersecurity plan contains several strategies. However, after the Omnibus and HITECH amendments, one of those strategies should include using an off-site data backup business associate. The increased CMPs, the four-tiered penalty analysis structure, the expanded definition of what constitutes a "breach," and the newly shared legal liability with business associates create numerous legal, functional, and policy benefits for health care providers that elect to have an off-site data backup. It appears Congress has granted the health care sector, through the Omnibus and HITECH amendments, an ally in business associates, particularly off-site data backup services. It is now left to providers to choose how to move forward in the war against ransomware and whether to utilize the benefits accessible from contracting with off-site data backup business associates.

JORDAN BUTLER*

They're Connected, Why They're Crucial, FLEXENTIAL (July 18, 2016), http://www.peak10.com/healthcare-encryption-hipaa-compliant-systems-how-theyre-connected-why-theyre-crucial/ (last visited Feb. 20, 2018).

* Bachelor of Arts in Political Science, William Jewell College; Juris Doctor, Saint Louis University School of Law (2018). The author thanks his advisor, Professor Robert Gatter, for his guidance throughout the writing of this comment. He also expresses his appreciation for the generous support of everyone on the journal as well as his friends and family.