Loyola Consumer Law Review

Volume 25 | Issue 4 Article 6

2013

HIPAA'S Influence on Consumers: Friend or Foe?

Anna Covert

HIPAA'S INFLUENCE ON CONSUMERS: FRIEND OR FOE?

Anna Covert

I. INTRODUCTION

The Health Insurance Portability and Accountability Act ("HIPAA") became effective on April 14, 2003[1] with the intention of protecting the privacy of individuals' health information by establishing minimum federal standards for safeguarding private information.[2] HIPAA governs covered entities including; healthcare providers, health plans, and healthcare clearinghouses, who may use and disclose personally identifiable health information of patients. HIPAA also provides for enforcement and sanctions when unauthorized disclosures occur.[3] HIPAA legislation is "national in scope, sweeping in its coverage, and far-reaching in its implications, and thus concerns a wide range of stakeholders."[4]

While HIPAA, in its entirety, seems to affect the healthcare industry positively, there are certain drawbacks. Namely, consumer needs can be adversely affected in multiple ways. For example, under the new regulation, there are ample opportunities for an interruption in sharing the health information "needed to

---

[1] Shannon H. Houser, *Assessing the Effects of the HIPAA Privacy Rule on Release of Patient Information by Healthcare Facilities,* 4 PERSP. HEALTH INFO. MGMT. 1, 1 (2007), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2082070/; *See also* Department of Health and Human Services Standards for Privacy of Individually Identifiable Health Information, 60Fed. Reg. (December 29, 2000), *available at* http://www.hhs.gov/ocr/hipaa/privacy.html.

[2] *Id.*

[3] *Id.*

[4] Elizabeth Asfaw, Health Insurance Portability and Accountability Act: Confidentiality and Privacy from the Perspectives of the Consumer and the Physician, 12 (March 2008) (unpublished Ph.D. dissertation, Capella University) (on file with ProQuest).

provide and promote high-quality healthcare in a timely fashion."[5] For instance, a delay might occur affecting the quality of healthcare in an emergency situation. Problems could arise when a patient is out-of-town and his medical records from his general practitioner are needed immediately but HIPAA provisions restrict the ability to transmit the necessary documents in a timely manner.

Another drawback that has been demonstrated since HIPAA's enactment is the costs of implementing the law. Not only are these costs a burden to the medical industry, but many costs have been passed onto consumers – making health services more expensive. Legislators recognize the drawbacks, and have attempted to address some of the inherent problems through amendments to the Act. It is critical to analyze how HIPAA and its amendments have and will continue to affect the industry because these effects trickle down raising concerns of which consumers should be aware.

HIPAA has received criticism from multiple healthcare industry professionals believing that it hinders, rather than opens, access to quality healthcare. This note will argue that, in order to increase healthcare quality, HIPAA needs more reform. There is a solid foundation to protect patients' healthcare information while maintaining quality care; however, changes in the regulation could increase the quality of care while limiting breaches of private health information and decreasing costs to customers.

In the next section of this note, I will discuss the history of HIPAA and why it was implemented. Section Three will focus briefly on the different regulations of HIPAA and their effects on the healthcare industry as a whole. Section Three will also delve into the cost of privacy, and whether HIPAA has accomplished its original goal. This section will focus on amendments and additions to the original HIPAA legislation, including the Health Information Technology for Economic and Clinical Health Act ("HITECH") enacted in 2009 and the HIPAA 5010 regulations, which required information technology departments to adjust infrastructure. Section Four will discuss HIPAA's costs – to consumers and to the healthcare industry. Finally, this note will discuss necessary, foreseeable future regulations.

---

[5] Houser, *supra* note 1.

II. WHY IS HIPAA NECESSARY?

A. Before HIPAA

Prior to the implementation of HIPAA, there was little regulation concerning the release of a patient's private information.[6] This was especially true regarding the use of computer and video technology in the distribution of health information.[7] The healthcare industry as a whole lacked policies regarding patient information distributed through these technologies.

Additionally, prior to HIPAA there was no uniformity in the protection of health information.[8] Instead, health information was mainly protected by a combination of "state laws, common law, and professional codes of ethical conduct."[9] The rules were not consistent across state borders and there was little enforcement mechanism in place. To this piecemeal system, HIPAA represents a "minimum, uniform standard of privacy on healthcare providers, which includes physicians and healthcare organizations."[10] In this sense HIPAA seemed to be a step in the right direction given the lack of uniformity of previous laws.

Modern changes in the ways individuals view their private life has had a huge affect on the medical industry and the perception of privacy issues. Patients today are extremely concerned with who has access to their information and what information is being accessed. The push for increased privacy emphasized the need for regulations of personal health information, and helped lead to the implementation of HIPAA.

In addition to privacy concerns, prior to HIPAA, if an individual lost his or her job and therefore, his or her insurance, then the next insurance company was able to classify the patient's needs as "pre-existing conditions."[11] This allowed the insurance

---

[6] *History of HIPAA,* ALL THINGS MEDICAL BILLING.COM, http://www.all-things-medical-billing.com/history-of-hipaa.html, 2012,(last visited April 18, 2013).

[7] *Id.* at 17.

[8] Ctr. for Democracy & Tech., *HIPAA and Health Privacy: Myths and Facts*, 2 (Jan. 2009), https://www.cdt.org/files/pdfs/20090109mythsfacts2.pdf.

[9] Asfaw, *supra* note 5, at 2.

[10] *Id.*

[11] BUS. DICTIONARY, http://www.businessdictionary.com/definition/job-lock.html.

provider to pay little or nothing for services needed to remedy such conditions, despite the fact that the client was (and had been) paying for insurance. HIPAA disallowed this policy, and instead required new companies to renew insurance policies and bars carriers from charging higher premiums based on health information, essentially making insurance coverage portable between companies.

The portability provisions are a significant advancement in the healthcare industry and extremely important for patients who can now safely leave their jobs or lose their jobs without the added stress of significant changes to their medical benefits.[12]

B. Provisions of HIPAA

Originally enacted in 1996, HIPAA was fully implemented in 2003.[13] This delay in enforcement occurred to give medical practices time to become compliant with the Act and to work out the many details of its provisions. The Office for Civil Rights ("OCR") is the entity responsible for enforcing these regulations.[14] Essentially, the Act has two goals; (1) to prevent "job lock," the inability of an employee to leave his or her job freely because of fear that he or she might lose the accompanying medical benefits, and (2) to protect the privacy of individually identifiable health information. [15]

Specifically, Title 1 of HIPAA provides insurance coverage protection for workers and families.[16] It protects employees with existing healthcare coverage from disqualification

---

[12] Letter from Andrew Sherill and John E. Dicken to the Honorable Harry Reid, the Honorable Max Baucus and the Honorable Tom Harkin (Dec. 15, 2011), *at* http://www.gao.gov/assets/590/586973.pdf.

[13] Sherry Holetzky, *What is HIPAA?,* WISEGEEK, http://www.wisegeek.com/what-is-hipaa.htm#.

[14] *HIPAA Enforcement,* HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/; *See also* Kala Ladenheim, *Health Insurance in Transition: The Health Insurance Portability and Accountability Act of 1996,* 27 PUBLIUS: J. AM. FED'ISM 33, 34 (1997), *available at* http://www.jstor.org.flagship.luc.edu/stable/3330636; See also Monica B. Wilkinson, *Impact of Consumer Privacy Rules from the HIPAA Perspective, available* at http://www.michbar.org/health/pdfs/hcHIPAAsmnr120302.pdf.

[15] Why Was HIPAA Created?, KNOWSWHY (March 7, 2011), http://www.knowswhy.com/why-was-hipaa-created/.

[16] *Id.*

of insurance benefits even if the worker loses his or her job, or changes careers.[17]

Title 2 of HIPAA, better known as the Administrative Simplification Act, requires the healthcare industry to become more efficient by encouraging the use of electronic media for transmission of certain patient administrative data.[18] To make the public feel more secure with the electronic transmission of data, the government developed privacy and security rules to complement the transaction rules.[19] Title 2 has five sections: Standards for Electronic Transactions, Unique Identifiers Standards, the Security Rule, the Privacy Rule, and the Enforcement Rule.[20]

The "Security Rule" is meant to ensure the protection of health information by establishing national standards for the security of Protected electronic Health Information ("PHI").[21] This section includes the "Patient Safety Rule," a set of rules designed to protect information from being used against the patient's desires.

The most important section of the Security Rule is the Department of Health and Human Services' ("HHS") requirement to create rules designed to increase effectiveness of the national healthcare system through established standardized policies. These policies concern distribution and utilization of healthcare related information. This section promotes the exchange of needed healthcare records among the United States' system through private and secure computerization.

---

[17] *Id.*

[18] *HIPAA Administrative Simplification Statute and Rules,* HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/administrative/; *See also,* Information Security Report, National Instituteof Standards and Technology, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

[19] *Id.*

[20] *Id.*

[21] Summary of th HIPAA Secutiry Rule, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html; See also, Information Security Report, National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, at vii-1, available at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Under the Final Security Rule, HIPAA makes a clear distinction between privacy and security by defining security as "covering electronic protected health information" and privacy as "covering all other PHI."[22] Essentially, security covers electronic data, while privacy considers non-electronic data. Prior to HIPAA, there was no need for this Security Rule.

Thus, the Privacy Rule, also under the Administrative Simplification Act, "covers PHI in any form it is created or received by a covered entity."[23] PHI is defined as "any oral or recorded information about the health of an individual, the provision of healthcare to the individual, or the payment for healthcare. . .that is individually identifiable."[24] For health information to be considered "individually identifiable," it must identify or reasonably be used to identify the individual.[25]

The Privacy Rule affects practically every person in the healthcare industry, including hospitals and healthcare providers.[26] This rule "addresses issues regarding patient access rights, rules for use and disclosure, new administrative requirements, and means for enforcement and compliance."[27] Personal health information transfers are supposed to be very private, and therefore, there is a need for trained professionals to transfer and handle these files since untrained employees can cause leaks of this private information. Therefore, Health Information Managers ("HIM") are key in implementing these changes. HIM's "acquire, analyze, and protect digital and traditional medical information vital to providing quality patient care."[28] All of these changes have transformed the way healthcare

---

[22] Asfaw, *supra* note 5, at 17.

[23] Patricia Anania Firouzan, *HIPAA Privacy Implementation Issues in Pennsylvania Healthcare Facilities,* 4 PERSP. HEALTH INF. MGMT. (2004), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2047323/.

[24] *Id.*

[25] *Id.*

[26] *Id. See also* Margret Amatayakul, *On the Fast Track to Privacy Rule Compliance*, 74(2) J. AHIMA, 16A-16D (2003); See also, Monica B. Wilkinson, *Impact of Consumer Privacy Rules from the HIPAA Perspective,* http://www.michbar.org/health/pdfs/hcHIPAAsmnr120302.pdf

[27] Firouzan, *supra* note 20.

[28] Brian E. Dixson, *A Roadmap for the Adoption of E-Health,* 5 E-SERVICE J. 1, 9, *available at* http://www.jstor.org.flagship.luc.edu/stable/pdfplus/10.2979/ESJ.2007.5.3.3.pdf.; *See also,* Xiaoming Zeng, *Redefining the Rule of Health Information Management Professionals in Health Information Technology,* PERSPEC. IN

organizations operate, and have shown that HIM's are key in facilitating these changes.[29] These managers are normally already in the medical field and have gone through training specifically for HIPAA compliance.

Additionally, HIPAA provides for three significant actions in the healthcare industry meant to create consistency and uniformity among healthcare facilities across counties and states. First, the Act grants HHS the authority to create uniform controls for the management and transfer of sensitive information, including the ability to determine which codes must be used to identify medical and administrative expenses.[30] Second, it creates a national identification system.[31] Finally, HHS was given the power to secure personal health information through the implementation of the Act.[32]

C. Some of HIPPA's Effects

1. Security Enhancements

The recent push for privacy in all aspects of transactions in the healthcare industry has effects on other areas of the

---

HEALTH INFO. MGMT., http://perspectives.ahima.org/redefining-the-roles-of-health-information-management-professionals-in-health-information-technology/#.UXDERo45c20

[29] Firouzan, *supra* note 20.

[30] *Id.* ("When asked if their facility had to adjust their current safeguards to meet this requirement, approximately 78 percent of facilities had to make adjustments to their administrative, technical, and physical safeguards to meet the HIPAA requirement.").

[31] National Provider Identifier Standard, CENTERS FOR MEDICARE AND MEDICAID SERVICES (April 5, 2013 at 10:45am), http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/NationalProvIdentStand/index.html?redirect=/nationalprovidentstand/ ; *See also, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

[32] Kala Ladenheim, *Health Insurance in Transition: The Health Insurance Portability and Accountability Act of 1996,* 27 PUBLIUS: J. AM. FED'ISM 33, 34 (1997), *available at* http://www.jstor.org.flagship.luc.edu/stable/3330636*; See also An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

management of a healthcare facility. For example, security must also be increased in order to provide for the necessary privacy. One author emphasizes this point:

> "Before HIPAA, traditional practices have emphasized openness rather than the hiding of information, and now hospitals, payors, and health systems will have to change the way they do business in order to increase privacy protections. Somewhat surprisingly, hospitals have in general remained wide open to visitors, patient advocates, and others on a round-the-clock basis and without nurses' stations or other health information areas becoming high security zones. This means that for hospitals, the security challenges are far greater than ever."[33]

2. Training Requirements

In order to ensure that the two primary goals of HIPAA are met; ((1)to ensure that people between jobs would still have access to quality healthcare coverage, and (2) to protect private health information and create a uniform standard for dispersing personal information), one thing HIPAA does is require that healthcare facilities stay in compliance with certain training elements.[34] This training teaches health industry employees what information is confidential, who has access to this information and when, how to handle this information to minimize breaches, and how to transfer this information to other healthcare professionals when these information transfers are appropriate.[35]

These requirements have been met by facilities through a number of different methods such as pamphlets, classes, and informal training workshops that can last between one and four hours.[36] All of these training requirements cost the organization

---

[33] Alan S. Goldberg, *HIPAA & Healthcare: A New Way of Sharing and Caring,* 2 (May 2, (2001), *available at* http://www.ehcca.com/presentations/ehc-info3/goldberg2.pdf.

[34] Health Information Portability and Accountability Act of 1996, Public Law 104-191, (1996), *available at* http://aspe.hhs.gov/admnsimp/pl104191.htm

[35] *HIPAA Privacy and Security Training(Updated),* AHIMA, http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048509.hcsp?dDocName=bok1_048509

[36] Firouzan, *supra* note 20.

time and money to implement and require hiring more attorneys and managers to interpret HIPAA and maintain compliance.[37]

III. HOW HIPAA HAS AFFECTED THE HEALTHCARE INDUSTRY

HIPAA represents an overhaul of the healthcare industry. The Act has increased regulation, augmented expenses for training and updating information technology systems, enforced compliance with the security provisions, and imposed fines and sanctions on violators under the HITECH 2009 provision (discussed below).[38]

The goals of HIPAA as determined in this note are hindered by multiple issues that, in some instances, were brought about by HIPAA itself. Therefore, there is still quite a bit of skepticism regarding this regulation. Many health professionals are concerned that HIPAA does more harm than good. One of the major concerns is that there are heavy fines and costs for minor "accidents" that release relatively unimportant, and unidentifiable private information. This has led to quite a bit of debate surrounding the implementation of HIPAA and what other legislation should occur surrounding compliance with HIPAA.

A. Changes Made By Health Information Management Professionals

The changes to the healthcare industry have been especially significant for Health Information Management professionals

---

[37] *Id.* (A 20-question survey was sent in the mail to HIM directors in Pennsylvania healthcare facilities to solicit feedback regarding implementation issues of the HIPAA privacy rule requirements. Questions focused on gathering basic demographic data, information on HIM involvement with the privacy rule requirements, the procedures whereby facilities were meeting the privacy rule requirements, occurrences of confidentiality breaches, and respondents' perceptions about the privacy rule. "[M]ore than half of respondents from hospitals with more than 400 beds saw the need to add additional HIM staff. Because the HIPAA act is so far reaching across an organization, perhaps staff at bigger facilities felt the need for additional HIM staff to ensure that all areas of the act were covered. A large number of respondents from large hospitals and mental and behavioral health facilities also saw the need for additional staff in the organization as a whole.").

[38] Houser, *supra* note 1.

and have required many changes for these individuals.[39] These professionals were tasked with the challenge of putting their respective health care facilities in compliance with the new regulations.[40] Challenges came from patients, media, and other healthcare providers.

Further, many professionals were left to interpret this Act themselves because there was little to no instruction as to how to implement these provisions on a daily basis.[41] This led to many different interpretations across the nation, which is contrary to what HIPAA was supposed to create, which is a uniform health policy. The regulation did not mention instructions or steps to follow to best implement these changes. The Act simply states a level of security that must be complied with and threatened sanctions for those who did not comply. The vague requirements left many HIMs in a frenzy to make changes, trying to stay in compliance before their organization was faced with these sanctions. The result was a myriad of interpretations of the imposed requirements across different healthcare organizations. These multiple interpretations mirrored the problems prior to HIPAA in which every state had its own health regulations.[42]

For example, a survey of HIPAA privacy implementation issues in Pennsylvania healthcare facilities revealed that the HIM's had a central role in both the implementation and the development of the policies that affected all healthcare professionals within their organization. Instead of relying on a clear mandate within the Act to describe what compliance was mandatory, HIM's across Pennsylvania reacted to the new law in individual and vastly variant ways, leading to multiple interpretations on the Act that is supposed to reach a national level.[43]

B. Problems Complying with HIPAA

While protecting privacy is important, there are other issues to consider, such as, reasons that medical information may need to be accessed in medical research, public health, and to

---

[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*

improve care overall.[44] Many physicians consider HIPAA regulations a "bureaucratic impediment" that does not actually protect and advance patient confidentiality.[45] This is especially the case in "incidental disclosures" where other healthcare workers happen to overhear conversations revealing PHI.[46]

The main source of problems regarding implementing HIPAA lies with vague language in key provisions of the Privacy Rule.[47] The language in this Rule left providers guessing what was actually permissible use of health information, and blurred the lines of what information fundraiser directors may gather from hospital records.[48] These ambiguities are expected to adversely affect the quality of healthcare that patients receive because more professionals are unclear as to what information is accessible and this leads to a lack of documentation.[49] Due to these adverse effects, some healthcare providers have become so restrictive that they either do not release any medical information or they choose to mail requested information rather than fax it (clearly an issue if immediacy is important). Providers have become more restrictive because they are afraid of fines, lawsuits, and media attention regarding any type of infringement. Many of these organizations choose to impose the most stringent restrictions simply because they cannot afford the significant fines and are unwilling to face criminal prosecution.[50]

Advancements in the industry have also caused concern regarding HIPAA implementation.[51] Recently, there has been a drive for integration, which combines formerly independent healthcare providers into "large health systems and networks that include many large and small providers, medical schools, ancillary services, technical support organizations, and similar providers of associated services."[52] This has led to many difficulties in implementation because these organizations are

---

[44] Asfaw, *supra* note 5, at 4.

[45] *Id.*

[46] *Id.*

[47] *Id.* at 5.

[48] Anne Clark, *Understanding the New 2013 HIPAA Healthcare Privacy Rules*, COLLINS GROUP, (Feb. 12, 2013), http://collinsgroup.com/donor-relations/understanding-the-new-2013-hipaa-healthcare-privacy-rules/.

[49] Asfaw, *supra* note 5.

[50] *Id.*

[51] *Id.*

[52] *Id.* at 18.

massive and this information travels to many sectors of this organization leading to more opportunities for breaches of personal health information. Health information has further been exposed due to the advancement of managed care organizations over recent years since this information is exposed to a wide range of business associates, all of whom have potential access to confidential information.[53] This information is now used more frequently when treating patients and when discussing future health plans since the information has become more readily available through electronic means.

C. HIPAA's Amendments

HIPAA has seen many amendments and additions since first being signed into law in 1996 that have attempted to solve some of these problems mentioned. This note will address some of the most significant amendments including the HITECH Act of 2009 and the HIPAA 5010 regulations.

The HITECH Act was implemented by the Office for Civil Rights and includes provisions regarding: "business associate liability; new limitations on the sale of protected health information, marketing, and fundraising communications; and stronger individual rights to access electronic medical records and restrict the disclosure of certain information."[54] HITECH also has rules regarding enforcement and breach notification. These provisions are extremely important because business associates are obligated to comply with the Security Rule's administrative, physical, and technical safeguard requirements.[55] HITECH enforces compliance with the security rule by administering higher fines and penalties for non-compliance. HITECH allows for criminal and civil sanctions to apply directly to the business associate along with the healthcare provider.[56]

---

[53] *Id.*

[54] United States Dep't of Health and Human Servs, Hitech Act Rulemaking and Implementation Update, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html.

[55] Kevin M. Kramer, *Business Associates, Be Hip to HIPAA: How Recent Changes in Law will Affect Your Company for Years to Come,* GIBBONS (May 5, 2009), http://www.gibbonslaw.com/news_publications/articles.php?action=display_publication&publication_id=2760.

[56] *Id.*

Under HITECH, civil penalties were increased to a range of $100 to $50,000 per violation, with a maximum penalty for additional violations in any one year ranging from $25,000 to $1,500,000.[57] Further, HHS is required to distribute portions of any civil penalties collected to the persons whose information was improperly disclosed or used, which could create a financial incentive for individuals to report suspected HIPAA violations.[58] HITECH requires a business associate to notify the covered entity upon discovery of a breach of unsecured PHI under its control, and then the covered entity must notify the impacted individual.[59] Notice of the breach must also be provided to HHS and prominent media outlets serving a particular area if more than 500 individuals in that area are impacted.[60] If fewer than 500 individuals are affected, the covered entity would still be required to maintain a log of breaches and submit it to HHS annually.[61] However, despite HITECH's implementation of these enforcement mechanisms, problems still arise with HIPAA privacy rules.

Another way in which the government has attempted to deal with problems associated with HIPAA is through the implementation of HIPAA 5010 transactions.[62] These 5010 transactions went into effect June 30, 2012 and require healthcare providers to adjust IT infrastructure and other processes – from appointment scheduling to legal collections – all of which

---

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] *Version 5010 Industry Resources*, CENTERS FOR MEDICARE & MEDICAID SERVS, , https://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/Versions5010andD0/Version_5010-Industry-Resources.html; *See also,* Judy Veazie, *Lessons Learned from 5010 to Remember for ICD-10*, 26 HEALTH CARE COLLECTOR 1, 6, *available at* https://1.next.westlaw.com/Document/I54801a1bf0df11e18b05fdf15589d8e8/View/FullText.html?navigationPath=Search%2Fv3%2Fsearch%2Fresults%2Fnavigation%2Fi0ad604040000013e2da12d872fbe391f%3FNav%3DANALYTICAL%26fragmentIdentifier%3DI54801a1bf0df11e18b05fdf15589d8e8%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=639d95f0104d4686bbacdcd98cdb3afe&list=ANALYTICAL&rank=3&grading=na&sessionScopeId=eae35c5f693119396dbd002bdd19e914&originationContext=Search%20Result&transitionType=SearchItem&contextData=%28sc.Search%29

encompass the revenue cycle, and cause costs to increase.[63] Prior to the 5010 transactions most hospitals were not reengineering revenue cycle workflows to capture information, such as claims submission, eligibility verification and prior authorization, meaning that insurers are anticipated to have a difficult time interpreting these new 5010 process flows and it will be costly to update these IT systems.[64] This may cause missing data requirements, technical glitches, and an increased number of pending or rejected claims, equating to significant payment delays.

While the 5010 regulations and the HITECH amendment have increased costs due to more individuals working on increasing the security level, these changes have made several improvements to the healthcare industry and businesses involved. The changes have improved claims accuracy, streamlined communication with payers, decreased days in accounts receivable, and boosted employee productivity and reduced costs.[65] These new implementations are pushing HIPAA in the right direction by causing business to overhaul the implementation measures used and giving more instruction on how to comply with HIPAA.[66]

However, even with all of the disadvantages of HIPAA there are also many benefits of personal privacy especially psychological benefits, which include protection of personal autonomy, supporting stable relationships with others, and personal development.[67] Privacy in the healthcare environment allows the patient to relax, emotionally vent, manage bodily

---

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] Judy Veazie, *Lessons Learned from 5010 to Remember for ICD-10*, 26 HEALTH CARE COLLECTOR 1, 6, *available at* https://1.next.westlaw.com/Document/I54801a1bf0df11e18b05fdf15589d8e8/View/FullText.html?navigationPath=Search%2Fv3%2Fsearch%2Fresults%2Fnavigation%2Fi0ad604040000013e2da12d872fbe391f%3FNav%3DANALYTICAL%26fragmentIdentifier%3DI54801a1bf0df11e18b05fdf15589d8e8%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=639d95f0104d4686bbacdcd98cdb3afe&list=ANALYTICAL&rank=3&grading=na&sessionScopeId=eae35c5f693119396dbd002bdd19e914&originationContext=Search%20Result&transitionType=SearchItem&contextData=%28sc.Search%29

[67] *Id.*

functions, and cope with loss, shock, and sorrow.[68] The main concern regarding psychological benefits if privacy is not protected "is the experience of being violated or invaded."[69] For these reasons the Privacy Rule "requires that individuals be informed of those persons authorized to access their protected health information and the persons to whom this information will be disclosed."[70]

IV. THE COSTS OF IMPLEMENTING HIPAA

HIPAA has raised fundamental issues "for healthcare providers, insurers, employers, policy makers, researchers, and, most prominently, for patients and consumers of healthcare services and their families"[71] This Act has inflated costs to the industry that are passed on to the consumer.[72] It has increased costs and bankrupted small healthcare providers, which may cause some large hospitals to form monopolies, which increases prices for consumers and gives consumers less options regarding their medical care.[73] Mandated disclosure audits by the government related to HIPAA have become burdensome on operations especially as HIM professionals try to be accountable, and document and control all facets of the release of private health information.[74]

Multiple problems with HIPAA still need to be addressed, such as the public's misunderstanding about the release of patient information, and the lack of an umbrella policy or regulation defining infractions and enforcement that allows individual institutions to make their own interpretations.[75]

Further, there is difficulty in following the rules, and finding qualified staff who can make decisions regarding the

---

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] Asfaw, *supra* note 5, at 12.

[72] Lisa Dorward, *The Positive and Negative Effects of HIPAA on Employment Laws,* THE HOUS. CHRONICLE, http://smallbusiness.chron.com/positive-negative-effects-hipaa-employment-laws-18500.html.

[73] *Id.*

[74] Carla Hogan, *HIPAA Will Have Impact on Employers,* THE BUSINESS REVIEW, http://www.bizjournals.com/albany/stories/2001/09/24/focus4.html?page=all.

[75] *Id.*

release of information with confidence. All are significant barriers affecting the release of information.[76] A common theme among these problems is the lack of knowledge of the new rules and conditions imposed by HIPAA.[77] "These observations may be a commentary on how loose and unrestrictive the conditions were before HIPAA."[78] Another major problem has been the loss of control by trained healthcare professionals when information technology personnel control some of the patient information found in electronic health records.[79] This phenomena leads to more individuals being informed of patients information generally, and the more individuals with access to PHI, the more likely a breach may occur. Additionally, these IT individuals might handle this information less delicately than a healthcare professional who understands the need for protecting the information.

The various interpretations of HIPAA guidelines contribute to delays in providing patient information to healthcare providers and other parties because different interpretations cause professionals to delay the rate at which the information is disclosed.[80] For example, patients may have their pertinent information withheld in emergencies, or they may be unable to give consent for procedures.

V. CONCLUSION

As articulated above, there are several problems with HIPAA, however, the ultimate solution to these problems is to clarify the law. There should be a more detailed explanation of the requirements under HIPAA so that HIM's can follow to create uniformity across healthcare organizations. Additionally, there should be more language in the law that addresses who should control patient information and how to handle patient information (especially in the hands of personnel who do not possess Health Information Management credentials.)[81] There is also a need for standardized instructions as to how to implement

---

[76] Houser, *supra* note 1.
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] Asfaw, *supra* note 5.
[81] Houser, *supra* note 1.

HIPAA and for extensive training of healthcare workers.[82] One possibility could even be that as electronic health records evolve to a paperless state, the disciplines of HIM and IT may of necessity merge, or HIM could be submerged or even eliminated within IT which would, in turn, restrict the number of individuals with access to this information and likely cut down on breaches.[83]

Individual physicians and hospitals also need to make adjustments.[84] Authorizations for the release of information need to be updated and revised along with the creation of new documents, such as a notice for patients regarding the use of their protected health information. Further, the more automated and electronically dependent the organization is, the greater the need to evaluate the security of the network infrastructure. This includes making sure code sets are up-to-date and the electronic transfer of data is protected. If billing is outsourced, then the billing company must be compliant as well because legal obligations cannot be outsourced under HIPAA.[85]

Generally, HIPAA is considered a step in the right direction regarding patient privacy, and it has resulted in more descriptive and detailed privacy policies; however, it has not improved the online privacy practices of these organizations.[86] While HIPAA is a solid foundation in protecting patients' healthcare information there is more work to be done as described in this note. There is a need for more clear interpretation of HIPAA to provide uniform compliance across the nation, and a need for a system where a limited number of individuals have access to health information. HIPAA has begun a very important process, but future legislation and enforcement will be needed to fully carry out the goals of HIPAA.

---

[82] *Id.*

[83] *Id.*

[84] Donna Bowers, *The Health Insurance Portability and Accountability Act: Is It Really All That Bad?, 14(4)* BAYL. UNIV. MED. CENT. PROC (Oct. 2001), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1305898/.

[85] *Id.*

[86] *Id.*