HIPAA VIOLATIONS

Student Name

Institutional affiliation

HIPAA Violations

The Health Insurance Portability and Accountability Act was implemented of 1996 by president Bill Clinton[1]. There are two titles of the act, and the first involves the protection of health insurance coverage for employees and their families if they are to lose or change their jobs. The second covers electronic healthcare transactions and the national standards of their implementation. Additionally, it illustrates the identifiers for health insurance plans, providers, and employers. Specifically, Title I of HIPAA monitors the breadth and availability of health care plans for groups. The act was an amendment of the Employee Retirement Income Security Act, the Internal Revenue Act, and the Public Health Service Act[2]. Title I of HIPAA mandates the coverage of employees and regulates the limitations that health care plans of groups may implement on the pre-existing conditions of the benefits. The plans have the possibility to reject some benefits within twelve months of enrollment in the plan or eighteen months if the individual is late.

Title I

The first title enables individuals to minimize the exclusion period by the time over which they were receiving credible coverage before their enrollment in the plan and following a significant break in coverage. The definition of "credible coverage" encompasses Medicare, Medicaid, and individual health plans. On the other hand, a significant break refers to a break of at least 63 days without receiving health coverage[3]. However, there are some exceptions that enable employers to tie co-payments or premiums to body mass index or use of tobacco. Title I does not include all healthcare plans as limited scope plans, such as vision or dental plans and long term health plans, are exempted from this clause. The limited scope plans are only applicable if they are part of the general plan. In essence, Title I illustrates five

[1] Annas, G. J. (2003). *HIPAA regulations-a new era of medical-record privacy?*.New England Journal of Medicine, *348*(15), 1486-1490.

[2] Ibid
[3] Ibid

categories for the calculation of continuous coverage. Finally, the Title does not include hidden exclusion clauses, and if these are present, they should be re-written.

Title II

As mentioned above, Title II aims to prevent abuse and healthcare fraud. Additionally, it seeks to simplify administrative processes through the definition of procedures, policies, and guidelines for the maintenance of security and privacy of health information that can be identified to specific individuals. Furthermore, Title II outlines different healthcare offenses and sets criminal and civil penalties for violations of them[4]. The title also controls several programs that oversee abuse and fraud within the healthcare system. The Department of Health and Human Services is necessary for Title II and drafts some regulations that improve the efficiency of the system through the creation of standards for dissemination and use of healthcare information. The rules are applicable to covered entities according to the HHS and the HIPAA[5]. These entities include health care clearing houses, health plans, community health information systems, billing services, and transmission of healthcare data in a way that adheres to the HIPAA regulations.

The HIPAA also has a privacy rule that regulates the disclosure and use of protected health information (PHI) within the covered entities. The Health and Human Services Department made an extension to the HIPAA rule, covering independent contractors that are within the bracket of business associates[6]. Protected Health Information refers to any data that relates to the health status of an individual, payment for health care, and provision of health care that can be connected to an individual. The interpretation of this term is broad and encompasses different attributes about a patient's information. There is also an obligation for covered entities to disclose PHI after request from an individual within thirty days of his or

[4] Centers For Disease Control and Prevention. (2003). *HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services*. MMWR: Morbidity and mortality weekly report, 52(Suppl. 1), 1-17.

[5] Ibid
[6] Ibid

her request. Furthermore, the disclosure of information should be done after requests by the law enforcement agencies in instances involving suspicion of criminal activities or child abuse. Additionally, law enforcement purposes, such as court ordered warrants, court orders, and subpoenas, suspicion of identity theft, missing persons, or material witnesses, mandate the disclosure of PHI.

The privacy rule provides people with the right to ask for the correction of any information that they feel may be erroneous. There is also a need for the providers of policies to take the necessary steps to protect private information of clients, and there should be confidentiality in the communicative processes with the individuals. Such protocols include specifics such as the phone number that an individual wishes to be used as their contact one or the address that may be used for the delivery of information. Individuals should also be notified every time their information is used, and the mentioned-above entities are required to keep a record of the disclosure of information and the procedures and privacy policies of the organization. Any individual that feels that there are violations in his or her privacy rules has the right to file a complaint.

HIPAA Compliance

HIPAA provides a set of standards that were mentioned above and sets standards for the protection of sensitive patient data. Therefore, any company that works with protected health information should ensure that the required network, physical, and process security measures are followed and in place. Compliance includes covered entities, which refers to all providers of treatment, payment, and/or other operations in healthcare[7]. Therefore, business associates or subcontractors and other organizations must all be in compliance with HIPAA regulations. Healthcare providers may stay in compliance of HIPAA regulations through

[7] Rorer, S. (2013). *Social Media Compliance Challenges: From HIPAA to the NLRA*. American Health Lawyers Association

certain physical, technical, and administrative safeguards implementation. The technical and physical safeguards are the most essential in the services from HIPAA compliant hosts. Technical safeguards mandate access control and ensure that only individuals that have authorization to access protected health data. There are different types of access control that include emergency access procedures, IDs, encryption and decryption, and automatic log off[8]. The physical safeguards include limitations in facility control and access, requiring some authorization for entrance. All the companies or covered entities that are in compliance with HIPAA regulations should have policies involving the access and use of electronic media and work stations. Finally, technical policies include the control of integrity and company measures that provide insurance that there was no violation of ePHI. There is also a need for IT recovery and data restoration policies to ensure that electronic failure and media errors are rectified immediately. In essence, compliance to HIPAA requires covered entities to adhere to different policies and principles that that ensure the protection of patient information. The compliance measures are applicable from different realms that include technical and physical measures.

Current and Potential Violations of HIPAA

As illustrated above, there are several barriers that may affect the adherence to the HIPAA. There is a range of common violations of HIPAA, and some famous examples include that of a company that left seventy-one boxes consisting of patients' medical records in Pennsylvania on the driveway. Another popular case that involved a celebrity is that of Britney Spears and the medical personnel that snooped on her records. One common violation is that of protected health information access. An example is a case that was investigated by the OCR, involving a mother of a minor who was denied access to the son's medical records. The actions of the provider were on the basis of state laws instead of federal

[8] Rorer, S. (2013). *Social Media Compliance Challenges: From HIPAA to the NLRA*. American Health Lawyers Association

regulations. The HIPAA suggests that the provider should provide the mother with full access to her child's records. In essence, when there is a contraindication between state and federal law, HIPAA takes precedence.

Authorization requirements of PHI are also an issue among healthcare providers. One of the issues that affect providers is when to release information to third parties, such as the employer. There are some parts of the act that allow the provision of information to these parties; however, it should only be done with the appropriate written consent. Many providers neglect this attribute of the clause as the attainment of authorization appears to be simple but is usually accompanied by many nuances. Another way that violation usually occurs is through business associate agreements. In some cases an organization that is associated with the provider may release information. In this aspect, it is the duty of the provider to ensure that the associate is fully aware of the privacy policy. There may also be violation of the act through communication as the provider may leave some information on the client's phone, which may be accessed by different people at home. The breach occurs when the client specifically asks for messages to be left on a private phone. In essence, there are several threats to the breach of HIPAA, and organizations should always exercise caution in their approaches with patient information. Some actions, such as communication or the attainment of authorization, may appear simple and straightforward. However, there are several challenges that could affect the privacy of patients, and companies should be cautious and prepared.

Protection against HIPAA

The penalties that may arise from the violation of privacy laws may range from a few hundred to millions of dollars. Hence, there is a need for a provider to take the necessary measures to protect themselves from the violation of HIPAA. The provider must take the necessary steps in ensuring that there is protection of all private records through safety

barriers that require access codes and restrict access. Secondly, there is a need to ensure that the data and needs of the patient are well documented, such as the preferable means of communication. It will allow the avoidance of information being incorrectly received by the wrong party. There is also a need to regulate the disposal of information and make sure that all unnecessary information is destroyed or shredded to ensure that no third party gains access. Third party disclosure policies are also important in the adherence to HIPAA. Prior to disclosing any information to a third party, the company must first contact the patient and ensure that he or she is aware of the process. Furthermore, there should be provision of written consent to avoid any misunderstandings in the future.

HIPAA and Media Sources

The use of websites and social media raises strains on organizations as they must adjust their policies and approaches to avoid violations of HIPAA. The majority of the organizations providing healthcare and their personnel, such as nurses, physicians, and other parties, are now communicating through social media, with the increase in the number of available platforms. These platforms include video sites, social networking sites, blogs, vlogs, online forums, and chatrooms[9]. In essence, the dilemma arises from the fact that social media is a popular platform for communication as the majority of individuals visit sites like Facebook on a daily basis. However, there are some difficulties in the sense that communication that is not cautiously carried out may result in the violation of HIPAA. The issue is further enhanced when there is sharing of patient specific communication[10]. Therefore, there is an issue in the sense that organizations need to create policies that regulate the amount of information that clients may receive on the social media.

---

[9] Rorer, S. (2013). *Social Media Compliance Challenges: From HIPAA to the NLRA*. American Health Lawyers Association

[10] Ibid

There are several current issues that have been experienced recently that involve the use of social media. An example is a group of students that took a photo of a shark attack victim during their training in an ED department of Martin Memorial Medical Center in Stuart, Florida. Another example is that of a physician who referred to his patient on his blog as ignorant and lazy. The reasons for these statements were that the patient visited the intensive care department as a result of failure to adhere to interventions that reduced her sugar levels. There are also several videos that are taken by students involving doctors performing different medical procedures on patients, such as insertion of tubes. Therefore, the different media sites increase the possibility of sharing information that may result in violation of the privacy act.

There are several methods that can be utilized reduce the occurrence of such activities. Firstly, there is a need to educate these professionals and scholars on the information that they are allowed to share. A survey illustrates that the majority of medical professionals are not aware of the constraints and the information they may share online. Secondly, there is a need for members of the healthcare community to regulate the use of devices during medical procedures. For example, students should not have the opportunity to take their phones into the classroom.

In 2009, President Obama signed the Health Information Technology for Economic and Clinical Health Act (HITECH), which resulted in the amendment of HIPAA in different ways[11]. As mentioned above, there are different factors that raise the challenges in adhering to the HIPAA. These include the fact that the violation itself is dependent on several factors, and the posting of information online is only a breech after identifying the purpose of the post and the target population. There is a need to acknowledge the fact that not all disclosures

[11] Nancy Spector PhD, R. N., & Kappel, D. M. (2012). *Guidelines for using electronic and social media: The regulatory perspective*. Online journal of issues in nursing, *17*(3), 1_11.

involving the release of health information are violation of HIPAA. The act is extensively fact sensitive as the healthcare provider has the possibility to release information to an individual that is directly related to the data[12]. Additionally, the provider is not required to receive any written consent from the candidate and the information can also be published without any permission or consent. However, the law is that the information should not be viewed by a third party if it is to adhere to HIPAA.

In the majority of cases, healthcare providers can disclose information of the patient without his or her consent to another covered entity or healthcare provider. The information may be provided for purposes of payment, healthcare operations, or treatment. Hence, if the network is secure to minimize the disclosure of data among and by physicians, platforms are applicable for use for different purposes, such as consultation regarding a particular patient and for training of staff, students, or residents[13]. Therefore, it illustrates that the exposure of information should follow some minimal parameters to ensure that the network is secure. For example, there could be creation of a closed group on Facebook, which requires the individual to scan their legal identification documents for permission to view information and interact with the group[14]. Furthermore, the private information may be sent exclusively through private messages to ensure that all members do not have access to all patients, except those that are necessary for their care provision.

As a result of the uncertainty that surrounds the communication platform, organizations should remain updated with the changes of regulatory parameters that surround patient information. For example, the past HIPAA requirements did not state that the organizations must notify the patients if there are any violations of the privacy rule in relation

[12] Ibid

[13] Moses, R. E., McNeese, L. G., Feld, L. D., & Feld, A. D. (2014). *Social media in the health-care setting: benefits but also a minefield of compliance and other legal issues*. The American journal of gastroenterology, *109*(8), 1128-1132.

[14] Ibid

to their data. However, the HITECH policy altered this clause and there should be notification after any form of breach[15]. The term refers to the access, disclosure, or acquisition of information that occurs in a way that is not permissible to HIPAA. The release of information is considered a breach if it results in the distribution of information that will place the patient or individual at risk in terms of his or her safety or reputation.

The use of social media and websites by providers is also increasing the number of people within the company that have access to information. Therefore, there is a need for these entities to ensure that the employees that have access to patient information are well educated in regards to the handling of data and making sure that they adhere to the HIPAA principles. Such individuals must also remain informed about any changes that occur in the act. The organization could ensure the process is efficient by offering training to its staff members and regular tests on the HIPAA policies. However, there are also some exceptions to the policies that provide entities with a life line in case the measures they take are unsuccessful. For example, if a staff member unintentionally discloses some information within the scope of his or her job responsibilities and in good faith, there is no breach. Nevertheless, the employees should be aware of the way to proceed following this realization. Information cannot continue to be used after the employee discovers that disclosure was in violation of privacy laws.

There are several other factors that come into play regarding the distribution of information that raise a need for intervention from an administrative perspective. For example, there was a case involving a NY Giants football player who wanted to sue ESPN for disclosing his medical information via the social media platform Twitter[16]. In particular, the information of his medical records stated that he had recently received an amputation of

---

[15] Ibid

[16] Hader, A. L., & Brown, E. D. (2010). LEGAL BRIEFS. Patient Privacy and Social Media. *AANA journal*, *78*(4).

his finger. The data published by the news network was from Jackson Memorial, where the two employees that were responsible for leaking the information were dismissed from their positions. Nevertheless, ESPN was not found in violation of the HIPAA because they are not a healthcare provider or a covered entity. Furthermore, the channel is protected by the First Amendment, which makes most experts state that such types of lawsuits are fruitless. Hence, the final arguments could be made regarding whether the information published was news worthy. Legally, when addressing information that is newsworthy, the press has the right to disclose the information regardless of the different privacy acts that exist. Therefore, it raises several questions as patients and community are vulnerable to such occurrences. The player may have emotional and financial implications as his reputation will be ruined and he may lose his job. Hence, there is a need to protect individuals in such situations as many people may gain access to private information in different methods. This information may then be released on social sites that the entire world may view. The implications of such procedures are limitless, and the law enforcement officials must place policies that create a balance between the privacy act and the ability for new networks to report an newsworthy information.

Avoiding HIPAA Violations on Social Media

There are numerous cases that have taken place involving HIPAA violations and social media and that raise a need for the appropriate intervention. Some authors suggest that it is not advisable to speak about patients even in general terms on social networks[17]. The use of patients as examples is ideal in the presentation of information and certain points; however, there are difficulties in creating anonymity of the individual in the example, and the process may lead to a breach of the privacy act. However, the providers may speak about

[17] Cain, J. (2011). *Social media in health care: the case for organizational policy and employee education*. American Journal of Health-System Pharmacy, *68*(11), 1036.

treatments, conditions, and other procedures used in patient care. Talking about a neutral perspective has an impact on the topic of discussion and avoids the utilization of private patient information.

Another approach that was suggested by Dr. Shay, who practices law in Philadelphia, is that entities should familiarize themselves with the different social networks. Becoming familiar with these networks allows physicians and their colleagues to take the necessary measures to avoid inappropriate sharing of information. Understanding the functions of the sites will also allow the individuals to explain to their staff the different measures that are necessary in their practice[18]. Many legal experts also advise against the inclusion of identification information on social networks. These individuals believe that removing such information in totality will avoid any unintentional disclosure. There are also studies that illustrate the poor security that exists on social networks. Hence, the organizations are vulnerable to hacking and unauthorized entry. Hence, it would be beneficial to the company and the client if the sharing of important information is only done through a secure communication network. The use of social media can be for non-protected information, such as consultations or some information regarding the policies of the company.

A study by Pew Research Center illustrates that approximately 60% of Americans utilize the internet to attain information on a particular drug or topic in relation to healthcare[19]. In a particular, a study entitled *The social life of health information, 2011* by Professor Fox illustrates that the Internet supersedes physicians as the first source of consult for health-related issues. Furthermore, the majority of people in the study view this source and the advice of their peers as reliable information. Hence, in the modern environment, it is

---

[18] Ibid

[19] Considine, M. (2013). *Exercising Caution Before Action: What Employers Need to Know Before Implementing the NLRB General Counsel's Approved Social Media Policy*. Hamline L. Rev., *36*, 517.

important to ensure that organizations adhere to HIPAA with their websites and social media pages and protect the coverage of their brand online as many people will have access to this information[20]. Social media creates a new and innovative method of engagement with patients, and the company should utilize the page as a way of spreading general information or tweeting notifications about some changes in policies. The entities should provide the patients with the opportunity to decide by themselves if they would like to follow the company or the doctor. Some organizations make the mistakes of adding patients or clients to their pages, which may raise some challenges as people may not be willing to be publicly associated with a provider for various reasons[21]. Allowing the patient to follow the physician ensures that he or she makes the decision regarding the information or data that he or she will like to share on his page.

Organizations may also take the approach of evaluating and placing some restrictions on the personal use of social media at work for communicating with a client or sharing work-related information. The staff should be restricted to the use of company pages for such process. It allows the entity to regulate the use of the page and the disclosure of information. Allowing \organizations to know the nature of social media use regarding work issues enables the implementation of the necessary policies to ensure that there is compliance with HIPAA and any violations are detected quickly and rectified. If \employees have access to social media or have the permission to use work information, they may be unintentionally sharing inappropriate information[22]. An example is that of the group of students that shared information of a shark attack victim. They may have done it for educational purposes or other aspects in good faith without the knowledge that they were violating the privacy rights of the patient. Therefore, it is necessary for companies to monitor their social networks and how the

[20] Ibid
[21] Ibid
[22] Green, A. C. (2012). *Using Social Networking to Discuss Work: NLRB Protection for Derogatory Employee Speech and Concerted Activity*. Berkeley Technology Law Journal, *27*, 837-889.

employees use them for the disclosure of information. It is also important to remind staff members that the use of smartphones and cameras should be in adherence with HIPAA and they should take their training into consideration[23]. However, the majority of scholars advice to ban the use of devices in the work place altogether. Some approaches that companies take are setting their networks to block the use of popular media sites, such as Twitter or Facebook, from personal gadgets. In short, it is important for staff and companies to take all factors into consideration as there are some challenges in the regulation of staff and personal use of social networks.

Online forums also pose a challenge to staff members as they may not be able to answer appropriately while concealing private information of the patient. As mentioned above, there are difficulties in maintenance of anonymity as individuals are often easy to identify after the presentation of their case. Therefore, entities should ensure that only individuals that are well trained can respond to questions or share data concerning the company on forums. There should be extensive training for these staff members, especially on language that is applicable and the information that is off limits for sharing.

Conclusion

There are several factors that contribute to the violations of and compliance with HIPAA. The use of social media makes it difficult to adhere to HIPAA policies as there is a possibility that information may be shared unintentionally. Additionally, there are many possible activities that individuals carry out under the false assumption that they are not breaching the act. Hence, there is a need for companies to adjust their policies to ensure that they adhere to HIPAA. The use of social network and media sources should be restricted to individuals that have extensive training in the field. The company should alter policies to ensure that the there is a strict protocol on the sharing of patient information. The majority of

[23] Ibid

authors state that it is advisable to avoid the sharing of such data on these sites and they should be utilized for promotion and notifications that do not involve personal information. The dilemma exists in the fact that the use of social networks continues to expand, and many people are utilizing this platform for communication. Nevertheless, the process is one of education and policy as companies may take measures to ensure that they reap the benefits of social media and websites and at the same time adhere to the policies of HIPAA.

References

Annas, G. J. (2003). *HIPAA regulations-a new era of medical-record privacy?*.New England Journal of Medicine, *348*(15), 1486-1490.

Cain, J. (2011). *Social media in health care: The case for organizational policy and employee education*. American Journal of Health-System Pharmacy, *68*(11), 1036.

Centers For Disease Control and Prevention. (2003). *HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services*. MMWR: Morbidity and mortality weekly report, 52(Suppl. 1), 1-17.

Considine, M. (2013). *Exercising caution before action: What employers need to know before implementing the NLRB General Counsel's approved social media policy*. Hamline L. Rev., *36*, 517.

Green, A. C. (2012). *Using social networking to discuss work: NLRB protection for derogatory employee speech and concerted activity*. Berkeley Technology Law Journal, *27*, 837-889.

Hader, A. L., & Brown, E. D. (2010). *Legal briefs. Patient privacy and social media*. AANA journal, *78*(4).

Moses, R. E., McNeese, L. G., Feld, L. D., & Feld, A. D. (2014). *Social media in the health care setting: Benefits but also a minefield of compliance and other legal issues*. The American journal of gastroenterology, *109*(8), 1128-1132.

Nancy Spector PhD, R. N., & Kappel, D. M. (2012). *Guidelines for using electronic and social media: The regulatory perspective*. Online journal of issues in nursing, *17*(3), 1_11.

Rorer, S. (2013). *Social media compliance challenges: From HIPAA to the NLRA*. American Health Lawyers Association