



This is a graded discussion: 4 points possible

Module 11 - Wednesday Discussion - March/April/May Discussion Group 2

The files of an estimated 75,000 individuals were accessed in a breach of Healthcare.gov for Affordable Care Act enrollment, according to the Centers for Medicare and Medicaid Services (<https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal> (<https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal>)).

As expected and with the need for secure patient information growing ever more critical, we need to be vigilant and proactive to prevent future attacks.

Using the March/April/May Discussion Groups, by Wednesday at the due time of 11:59 pm, each student posts his/her view of the threat and proposed actions to prevent it in the March/April/May discussion groups.

No more than 250 words per post, although you can use multiple posts to finish your answer if necessary.

Reminder: Formal writing; use APA style; cite your sources.



← Reply



Module 11: Wednesday Discussion

Personal Health Records (PHR) open new opportunities for enhancing delivery of standard health care services and health information to general population and supporting individuals to take more active role in health management and decision-making processes. This makes the healthcare industry a prime target for cybercriminals due to the large amount of high-sensitive patient information that can be accessed which includes date of birth, social security number and current and previous addresses – all of which can be used to steal a person's identity (Mirkovic et al.,2015). In traditional healthcare systems, the health information exchange was primarily paper-based and it is highly inefficient. Recent advances in technologies such as cloud computing, communication, mobile technology as well as satellite technologies allowed the development of e-health solutions providing a means for efficient sharing of health resources and making it a part of day to day life of general public. Such systems intend to provide healthcare services with high efficiency and flexibility while establishing a platform for secure sharing of health related data across different healthcare settings and work-flows among different healthcare providers (Pussewalage et al.,2016). Cloud computing can also allow data to be shared across multiple systems, which is lacking in many current healthcare facilities. Doctor's references, prescriptions, EHR and diagnoses could all be shared over various systems by cloud computing (Ali et al.,2018).

It is imperative that healthcare organizations take steps to reduce the possibility of a data breach:

1. Conduct an Annual security risk analysis: The HIPAA Security Rule requires periodic risk analysis already. This analysis will help to identify vulnerabilities and the possible areas of improvement. Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail.
2. Limit access to patient information:Users should only have access to patient healthcare data that relates to their position. Restricting access and managing user permissions are essential components of preventing a healthcare data breach (Clason et al.,2018).



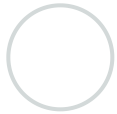
I agree that a great security measure is to limit how much data each user can access. This abides with the minimum necessary rule imposed by HIPAA (Roach, 2000). I found an

article that describes how blockchain can be used to allow access to resources. Specifically, the right is stored within the blocks of the blockchain, and allows users to view data with or without the right to tamper with it. The right to access can also be held by one user at a time, and are easily transferable (Maesa, Mori, & Ricci, 2017). Overall, I think the adoption of blockchain for user access is a great idea and may be implemented by multiple institutions in the future.

Maesa, D. D. F., Mori, P., & Ricci, L. (2017, June). Blockchain based access control. In *IFIP International Conference on Distributed Applications and Interoperable Systems* (pp. 206-220). Springer, Cham.

Roach, M. C. (2000). HIPAA privacy: "individual rights" and the "minimum necessary" requirements. *Journal of Health Law*, 33(4), 549-582.

← Reply



3. Blockchain platform ensures that your data is encrypted, which means that modification in data is a difficult task. Since blockchain as a technology is decentralized in nature it does not rely on one central point of control. It is a digital ledger of transactions with every computer having a complete copy of the data. As the name implies blockchain is a chain of digital “blocks” that contain records of transactions. (Pussewalage et al., 2017).

4. A symmetric cryptosystem uses only one key for both encryption and decryption of the data. The key used for encryption and decryption is called the private key and only people who are authorized for the encryption/decryption would know it. (Wright & Sittig, 2007).

References:

Mirkovic, J., Skipenes, E., Christiansen, E. K., & Bryhni, H. (2015). Security and privacy legislation guidelines for developing personal health records. *2015 Second International Conference on EDemocracy & EGovernment (ICEDEG)*. doi: 10.1109/icedeg.2015.7114460

Pussewalage, H. S. G., & Oleschuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6), 1161–1173. doi: 10.1016/j.ijinfomgt.2016.07.006

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146–158. doi: 10.1016/j.ijinfomgt.2018.07.009

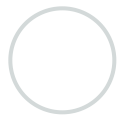
Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: *Blockchain in Healthcare Today*. doi: 10.30953/bhty.v1.20

Pussewalage, H. S. G., & Oleshchuk, V. A. (2017). Attribute based access control scheme with controlled access delegation for collaborative E-health environments. *Journal of Information Security and Applications*, 37, 50–64. doi: 10.1016/j.jisa.2017.10.004

Wright, A., & Sittig, D. F. (2007). Encryption Characteristics of Two USB-based Personal Health Record Devices. *Journal of the American Medical Informatics Association*, 14(4), 397–399. doi: 10.1197/jamia.m2352

← [Reply](#)

- -



Wednesday Discussion Post

I believe that data breaches should be taken very seriously. Security and privacy threats are common across multiple institutions. In 2005, over 22 million privacy violations had been reported by the Privacy Rights Clearinghouse (Pussewalage & Oleshchuk, 2016). The data obtained in breaches by hackers contributes to the profits made on the black market. Counterfeit medicines produce \$200 billion per year (Clauson, Breeden, Davidson, & Mackey, 2018). In regard to the CMS case, not only did the breach affect a vast amount of individuals, but the quantity of information taken and the method of access is unknown (Centers for Medicare & Medicaid Services, 2018). Therefore, I believe the threat must be taken seriously to protect the privacy of the individuals at hand.

My suggestion to prevent future threats from happening is to adopt blockchain technology with cloud computing. Blockchain functions by using a decentralized network with multiple computers acting as nodes. Because each node contains or owns the data, it becomes immutable, which makes it very resistant to fraud. This also increases the reliability of the data (Kaur, Alam, Jameel, Mourya, & Chang, 2018).

← [Reply](#)

- -

Cloud computing is predicted to be used by 80% of companies this year. Benefits of cloud computing include having readily available IT support, usability at locations that don't have onsite infrastructures, and increased capabilities of data sharing (Ali, Shrestha, Soar, & Wamba, 2018). Cloud computing and a blockchain platform work well together and can be used for managing access to important health data (Kaur, Alam, Jameel, Mourya, & Chang, 2018).

It is important for privacy and security systems to maintain an equilibrium between effectiveness and usability (Pussewalage & Oleshchuk, 2016). Cloud computing offers a usable platform for many organizations, while blockchain technology offers an effective security system for maintaining privacy of PHI.

References

Ali, O., Shrestha, A., Soar, J., & Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158. <https://doi.org/10.1016/j.ijinfomgt.2018.07.009>

Centers for Medicare & Medicaid Services (2018, October 19). *CMS Responding to Suspicious Activity in Agent and Broker Exchanges Portal*. CMS.gov. <https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal>

Clauson, K.A., Breeden, E.A., Davidson, C., & Mackey, T.K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain in Healthcare Today*, 1, 1-12. <https://doi.org/10.30953/bhty.v1.20>

Kaur, H., Alam, M. A., Jameel, R., Mourya, A. K., & Chang, V. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *Journal of Medical Systems*, 42(8), 156.

Pussewalage, H.S.G., & Oleshchuk, V.A. (2016). Privacy-preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6B), 1161-1173. <http://dx.doi.org/10.1016/j.ijinfomgt.2016.07.006>

 [Reply](#)

Yesterday

Hii Anna,

The point you mentioned regarding block chain technology and remote nodes was quite interesting. I have gone through the article and understood a few technological aspects in detail. (Kaur, Alam, Jameel, Mourya, & Chang, 2018). I have come across some technologies like Public key encryption, symmetric key based mechanism with smart cards and contract-oriented mechanisms, threshold cryptography mechanisms, systems incorporated with PKE and systemic cryptosystems which can be used to enhance security. [Pussewalage, H.S.G., & Oleshchuk, V.A. (2016)]. While all the attempts of encryption are being outdated with the hackers being updated at each security control.

← Reply



Anna,

I also support cloud computing as an intervention health informatics must adopt to fix challenges today. However, I do have some hesitation. "Cloud computing service delivery is prone to poor encryption key management, public management interface and separation failure" (Ali, Shrestha, Soar, & Wamba, 2018). The previous article also go on to mention how threats are more challenging to solve that convention IT systems. While I do support our need to adopt cloud computing there are fears to address. Have you come across any specific concern about cloud computing in your research?

References

Ali, O., Shrestha, A., Soar, J., & Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158.
<https://doi.org/10.1016/j.ijinfomgt.2018.07.009>

← Reply



The CMS report estimating that 75,000 individuals were involved in a data breach in 2018 is scary and I agree that ensuring the security of healthcare information is of utmost importance especially in the current era of electronic health records (EHR) and prevailing communication of confidential data (CMS.gov, 2018). Data breaches are not uncommon, and under the HITECH Act, breaches involving 500 persons or more should be reported to the secretary of human and health services, and data is publicly present in their web portal (U.S. Department of Health and Human Services, 2020). Upon reviewing this website, it is clear that data breaches are common, occurring almost daily and involving many states in the USA. The United States is continuing to support the initiative of adopting EHR instead of hand-written clinical data, this was initially suggested by the institute of medicine (Gardiyawasam Pussewalage & Oleshchuk, 2016, p. 1162; Gunter & Terry, 2005, pp. 1-2).

[← Reply](#)



Electronic exchange of data is important and prevalent in healthcare and cloud computing is evolving rapidly, yet, it imposes a security threat of being breached (Ali et al., 2018, p. 147). To secure this data, different keys can be used, the symmetric key utilizes the same one to encrypt and decrypt the data which is efficient but imposes security threats when the key is being transferred from the sender to the recipient (Gardiyawasam Pussewalage & Oleshchuk, 2016, p. 1163). On the other hand, public-key encryption uses two keys, a public key to encrypt the data which is publicly available as denoted by its name, and a private key to decrypt the data. This method is less efficient, yet, provides improved security standard which is important to ensure the security of the transferred data (Gardiyawasam Pussewalage & Oleshchuk, 2016, p. 1163). Blockchain technology is gaining increased popularity in healthcare systems as it reduces the risk of hacking, offers easier tracking, improves accuracy, reduced costs by eliminating third-party verification (Clauson et al., 2018, p. 8). Also, controlling access to healthcare records and keeping a detailed chronological logs using audit trails is critical to maintain it (Rostad & Edsberg, 2006, p. 8).

In conclusion, maintaining the security of healthcare data is very important, various tools are available to prevent unauthorized access and manipulation.

References

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158.

<https://doi.org/10.1016/j.ijinfomgt.2018.07.009>

[_ \(https://doi.org/10.1016/j.ijinfomgt.2018.07.009\)](https://doi.org/10.1016/j.ijinfomgt.2018.07.009)

Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare.

Blockchain in Healthcare Today, 1, 1-12. <https://doi.org/10.30953/bhty.v1.20>

[_ \(https://doi.org/10.30953/bhty.v1.20\)](https://doi.org/10.30953/bhty.v1.20)

CMS.gov, Centers for Medicare & Medicaid Service (2018, Oct 19). *CMS responding to suspicious activity in agent and broker exchanges portal*. Retrieved April 8, 2020

from [https://www.cms.gov/newsroom/press-releases/cms-responding-](https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal)

[suspicious-activity-agent-and-broker-exchanges-portal](https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal)

[_ \(https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal\)](https://www.cms.gov/newsroom/press-releases/cms-responding-suspicious-activity-agent-and-broker-exchanges-portal)

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6), 1161-1173.

<https://doi.org/10.1016/j.ijinfomgt.2016.07.006>

[_ \(https://doi.org/10.1016/j.ijinfomgt.2016.07.006\)](https://doi.org/10.1016/j.ijinfomgt.2016.07.006)

Gunter, T. D., & Terry, N. P. (2005, Mar 14). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research*, 7(1), e3.

<https://doi.org/10.2196/jmir.7.1.e3> [_ \(https://doi.org/10.2196/jmir.7.1.e3\)](https://doi.org/10.2196/jmir.7.1.e3)

Rostad, L., & Edsberg, O. (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. 2006 22nd Annual Computer Security Applications Conference (ACSAC'06), (pp. 175-186). IEEE.

U.S. Department of Health and Human Services, O. f. C. R. (2020). *Breach portal: Notice to the secretary of HHS breach of unsecured protected health information*.

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

(https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

← [Reply](#)



My personal view of this threat is that this violation of security and privacy will not be a secluded case and steps must be taken to address security issues or healthcare informatics will be unable to advance. Health information technology is under constant threat from hackers, user misuse, and network breakdowns (Ali, Shrestha, Soar, & Wamba, 2018). Healthcare has strict security regulatory requirements concerning patient data due to HIPAA and HITECH. This breach will result in a review of the Centers for Medicare and Medicaid Services' (CMS) patient health information security. The CMS will be penalized for whatever HIPAA and HITECH factors they did not comply with. Ultimately this breach will require a risk analysis to be performed and the CMS will need to implement a plan to address their security issues (HIPAA, 2020).

← [Reply](#)



My proposed action plan would be to utilize cloud storage and implement an attribute base encryption (ABE) driven mechanism and use Blockchain techniques to improve security and privacy. Around 31% of the healthcare sector utilizes cloud storage at this moment and it is predicted that most other health associations will use this tool in the next 5 years (Ali et al., 2018). Cloud storage will become the go to method in upcoming years due to its cost efficiency and ability to share data across multiple systems (Ali et al., 2018). To ensure this system change will be the most beneficial, the system should begin the process to switch to cloud storage. The next decision should be how to protect the data used in this storage. According to Pussewalage & Oleshcuk, "it is evident that existing ABE based mechanisms...sustain superior privacy levels" (2016). To improve the ABE mechanisms, Blockchain can be drawn into the authorization of devices used by the CMS. By utilizing a Unique Device Identifier (UDI), "blockchain has the potential to reduce costs and improve patient safety...due to its efficiencies and accountability (Clauson, Breeden,

Davidson, & Mackey, 2018). Devices used in healthcare have been shown to be potential avenues for hackers to gather user data (Clauson et al., 2018). Utilizing blockchain can protect the CMS from breaches through these methods.

← Reply



References

Ali, O., Shrestha, A., Soar, J., & Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158.

<https://doi.org/10.1016/j.ijinfomgt.2018.07.009>

Clauson, K.A., Breeden, E.A., Davidson, C., & Mackey, T.K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare.

Blockchain in Healthcare Today, 1, 1-12. <https://doi.org/10.30953/bhty.v1.20>

HIPAA Journal. (2020, February 10). What are the Penalties for HIPAA Violations? Retrieved April 8, 2020, from <https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/>

Pussewalage, H.S.G., & Oleshchuk, V.A. (2016). Privacy-preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6B), 1161-1173.

<http://dx.doi.org/10.1016/j.ijinfomgt.2016.07.006>

← Reply

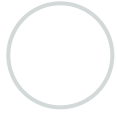


Hi Samuel,

Cloud is a major data storage system of present day and slowly it is being adapted by the health care portals. With the increased dependency over cloud has been attracting technological personnel like health IT professional to investigate them keenly for all the possible ways it could be misused and the data

be stolen. If proper laws and regulations have been implemented by the governing bodies of health care systems and taken seriously as a crime, it would provide some concrete outlines which people would be afraid to cross. What would you feel.

[← Reply](#)



CMS is a popular organization and no doubt data breach would be a unerasable remark over them. Though 75,000 is a small number compared to the number of customers CMS has, It is the quality to be considered rather than the quantity in such cases. From my understanding there was a breach in the Direct Enrolment pathway for agents and brokers. The first step after the breach was to prevent this from happening further and for this, they deactivated the accounts and disabled the agents and brokers suspected. (CMS, 2018). Later the extent of the breach needs to be calculated for which HIPAA security and privacy guidelines are to be followed. Before the implementation of any new feature to the portal careful analysis is to be done which authenticates the freshly installed features abide and are in unison with rules, regulations and policies as explained with HIPPA in order to prevent data breaches rather than trying to resolve it after. (Ammenwerth. E., S. Gräber, Herrmann, G., Burkle, T., &Konig, J., 2003).

Several methods of security and confidentiality include Public key encryption, symmetric key based mechanism with smart cards and contract-oriented mechanisms, threshold cryptography mechanisms, systems incorporated with PKE and systemic cryptosystems which can be used to enhance security. [Pussewalage, H.S.G., & Oleshchuk, V.A. (2016)].

[← Reply](#)



Biometry like retina scan, fingerprint scan and facial recognition technology can be used to further enhance the security. Dual authentication is a well-known practice where the user has

two barriers placed to prevent access by unauthorized if the hacker can decode one, he still has another barrier to prevent his entry. [Clauson et. Al. (2018)].

Cloud computing providers must be selected carefully as it could possess some hidden data breaches, leading to privacy threats. The bright side of medical decision making compels us to be attracted to it. The loss of control on data management by CMS need to be carefully evaluated by the regulations governing the healthcare sector. [Ali et al. (2018)]. Supporting It Mirkovic et al. (2015), have identified and evaluated the Laws and Regulations related to security of sensitive health data.

References:

U.S. Centers for Medicare & Medicaid Services. (2018). CMS responding to suspicious activity in agent and broker exchanges portal. Retrieved from <https://www.cms.gov/newsroom/press-releases/cms-responding-suspiciousactivity-agent-and-broker-exchanges-portal>

Ammenwerth, E., S.Gräber, Herrmann, G., Burkle, T., &Konig, J. (2003). Evaluation of health information systems—problems and challenges. Preview the document International Journal of Medical Informatics, 71(2-3), 125-135. Retrieved from <https://www.ncbi.nlm.nih.gov/pubmed/14519405>

Pussewalage, H.S.G., & Oleshchuk, V.A. (2016). Privacy-preserving mechanisms for enforcing security and privacy requirements in E-health solutions.Preview the document International Journal of Information Management, 36(6B), 1161-1173. <http://dx.doi.org/10.1016/j.ijinfomgt.2016.07.006>

Clauson, K.A., Breeden, E.A., Davidson, C., & Mackey, T.K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare.Preview the document Blockchain in Healthcare Today, 1, 1-12. <https://doi.org/10.30953/bhty.v1.20> (Links to an external site.)

Ali, O., Shrestha, A., Soar, J., & Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. Preview the documentInternational Journal of Information Management, 43, 146-158. <https://doi.org/10.1016/j.ijinfomgt.2018.07.009>

Mirkovic, J., Skipenes, E., Christiansen, E.K., & Bryhni, H. (2015, April). Security and privacy legislation guidelines for developing personal health records. Preview the document 2015 Second International Conference on EDemocracy & EGovernment (ICEDEG), 77-84. doi: 10.1109/icedeg.2015.7114460

← [Reply](#)



Hi Gopala,

I agree to the points you mentioned like retina scan, fingerprint scan and facial recognition technology can be used to further enhance the security (Clauson et al., 2018). This has some hidden risks associated to it. Fingerprints and facial scans are seen as an enhanced additional layer of security, but they rely on database storage just like any other type of data. Unlike a stolen password, biometrics data cannot be changed and could provide an attacker with physical access to buildings. Recently a security breach including the leak of personal information on 80 million Americans was discovered by security researchers in BioStar 2 which is a Supreme web-based security platform that is used throughout the world (Ikeda & Scott., 2019)

References:

Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: *Blockchain in Healthcare Today*. doi: 10.30953/bhty.v1.20

Ikeda, S. (2019, August 24). Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data. Retrieved from <https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/>

← [Reply](#)



bella.rose225 (my post)



Anytime you have a hole in security, and patient data gets out, it's a challenging situation. The consequence of the security breaches in health care reaches beyond the concealment of the data. The security breaches can lead to interruption of patient care, improper treatment, which could be caused by unfinished loss of data or full loss of data or lack of data availability, separation to insurance services that could gain impact patient care. Ensuring the protection of healthcare information is of very important, especially in the current period of electronic health records (EHR) and regular communication of confidential data (U.S. Centers for Medicare & Medicaid Services, 2018). Data breaches should be taken very seriously. Multiple institutions experience security and privacy threats.

Even though 75000 is not a significant fraction of patient records, but when it comes to data being exploited, any system breach is a huge impact and is not acceptable. We should concentrate on having a proper interface as well as employment security to counter any compromise on the patient's records in the first place. One of the most dependable ways is to have encryption to guard the patient's data in case of any cyber-attack or if someone has gained access to our internal data systems. All the organizations should emphasize critically on taking security training to instruct the workers with the proper use and handling of PHI. These steps, if taken appropriately, will help reduce security incidents.

← [Reply](#)



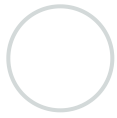
References:

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146–158. doi: 10.1016/j.ijinfomgt.2018.07.009

Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain in Healthcare Today*, 1, 1-12. <https://doi.org/10.30953/bhty.v1.20>

U.S. Centers for Medicare & Medicaid Services. (2018). CMS responding to suspicious activity in agent and broker exchanges portal. Retrieved from <https://www.cms.gov/newsroom/press-releases/cms-responding-suspiciousactivity-agent-and-broker-exchanges-portal>

← [Reply](#)



Friday Response

All group members believed the CMS security breach to be a threat. They stated how data breaches are commonplace and that threats are constant due to the presence of hackers, misuse by users, and possibility of networks being compromised (Ali, Shrestha, Soar, & Wamba, 2018). One group member brought up a great point that the severity of the threat is dependent on the quality rather than quantity of data stolen. None of the group members believed the threat should be overlooked or not taken seriously.

Many options were suggested for how to prevent security threats. The most common suggestion was to enforce encryption. Symmetric key encryption and public-key encryption were explained as being easier to use versus higher security protection respectively. Attribute based encryption is seen as superior method for protecting privacy (Gardiyawasam, Pussewalage, & Oleshchuk, 2016). Blockchain technology was another common suggestion. This was recommended due to its decreased hacking risk, ease of following data, and reduced costs (Clauson, Breeden, Davidson, & Mackey, 2018). The last action mentioned by multiple group members that I believe to be a good solution is enforcing risk analyses. These are required by the HIPAA Security Rule and helps detect vulnerabilities before an attack happens (Hash, Bowen, Johnson, Smith, & Steinberg, 2005).

← Reply

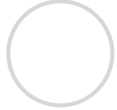


References

- Ali, O., Shrestha, A., Soar, J., & Wamba, S.F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146-158. <https://doi.org/10.1016/j.ijinfomgt.2018.07.009>
- Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6), 1161-1173. <https://doi.org/10.1016/j.ijinfomgt.2016.07.006>
- Hash, J., Bowen, P., Johnson, A., Smith, C. D., & Steinberg, D. I. (2005). *An introductory resource guide for implementing the health insurance portability and accountability act*

(HIPAA) security rule. US Department of Commerce, Technology Administration, National Institute of Standards and Technology

← Reply



Friday Discussion

All team members agreed that Security breach is one of the threats Americans face nowadays. There are many causes for a data breach such as weak and stolen credentials, Application vulnerabilities, Malware, Malicious insiders etc (Ali et al.,2018). Healthcare industry a prime target for cybercriminals due to the large amount of high-sensitive patient information that can be accessed which includes date of birth, social security number and current and previous addresses – all of which can be used to steal a person's identity (Mirkovic et al.,2015). Many points were suggested by the team members to reduce the possibility of a data breach. Out of which I found three quite promising:

Blockchain is far more secure than other record keeping systems because each new transaction is encrypted and linked to the previous transaction. It is formed by a complicated string of mathematical numbers and is impossible to be altered once formed. This immutable and incorruptible nature of blockchain makes it safe from falsified information and hacks (Clason et al.,2018). Another way to prevent data breaches is to enforce encryption such as the attribute-based encryption, symmetric key encryption and public key encryption. This is the method by which information is converted into secret code that hides the information's true meaning (Pussewalage et al.,2016). Enforcing risk analysis is very important and this can be achieved by the HIPAA security rule and this can help to detect the treats even before something goes wrong (HIPAA.,2020).

References

- Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146–158. doi: 10.1016/j.ijinfomgt.2018.07.009
- Mirkovic, J., Skipenes, E., Christiansen, E. K., & Bryhni, H. (2015). Security and privacy legislation guidelines for developing personal health records. *2015 Second International Conference on EDemocracy & EGovernment (ICEDEG)*. doi: 10.1109/icedeg.2015.7114460

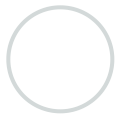
Clauson, K. A., Breeden, E. A., Davidson, C., & Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: *Blockchain in Healthcare Today*. doi: 10.30953/bhty.v1.20

Pussewalage, H. S. G., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6), 1161–1173. doi: 10.1016/j.ijinfomgt.2016.07.006

HIPAA Journal. (2020, February 10). What are the Penalties for HIPAA Violations? Retrieved April 10, 2020, from <https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/>

← [Reply](#)

- -



Friday Response: Critically summarizes the postings and then proposes the 3 most promising actions

All member in this discussion agreed that breach of the Centers for Medicare and Medicaid Services was indeed a threat to consider. These breaches are not uncommon as health information is valuable data. Rhema specifically mentions how patient health records possess date of birth, social security number, among other data pieces that can be used to steal a person's identity (Mirkovic, Skipenes, Christiansen, & Bryhni, 2015). Although all agreed step must be taken to address this threat, there were different ideas on how best to do so. Three users discussed the value Blockchain adds to security. All but one user praised the necessity for some sort of encryption. Although there was no consensus for what encryption tool to use, many were passionate about the tool they selected. Michael specifically supported public-key encryption, which uses a private key to decrypt data. Michael references Gardiyawasam, Pussewalage, & Oleshchuk as they explain how public-key encryption is an improved security standard and increases security for transferred data (2016). Most users also promoted the benefits that would come with incorporating cloud storage. The three most promising actions to improve security in this discussion are Blockchain, some method of encryption, and cloud storage.

References

Gardiyawasam Pussewalage, H. S., & Oleshchuk, V. A. (2016). Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management*, 36(6), 1161-1173.
<https://doi.org/10.1016/j.ijinfomgt.2016.07.006>

Mirkovic, J., Skipenes, E., Christiansen, E. K., & Bryhni, H. (2015). Security and privacy legislation guidelines for developing personal health records. *2015 Second International Conference on EDemocracy & EGovernment (ICEDEG)*. doi: 10.1109/icedeg.2015.7114460

 Reply