HIPAA (Health Insurance Portability and Accountability) compliance can help minimize a data breach when implementing encryption by identifying Personal Health Information (PHI) such as what your organization creates, receives, transmits, and stores (HIPAA Journal, 2018). Also, according to (HIPAA Journal, 2018) it can help your organization “identify human, natural, and environmental threats to the integrity of PHI.” After implementing encryption, the HIPAA compliance helps by using technical safeguards to make sure anyone accessing the PHI according to (HIPAA Journal, 2018) is who they say they are, that they do what they are supposed to do; and if an issue is present due to an accidental or malicious action, the issue is identified and rectified at the earliest possible opportunity. According to (NORCAL Risk Management, 2018) the best way to avoid HIPAA data breach is by using strong encryption. Using encryption gives the data a low probability of anyone other than the intended party will be able to decrypt it, due to the private key (NORCAL Risk Management, 2018). HIPAA compliance defines encryption in which there is low probability of assigning meaning without the confidential process or key. Also, data at rest and data in motion are addressed separately in the HIPAA encryption guidance which uses the NIST (National Institute of Standards and Technology) publications. The NIST publications will help the organizations comply with the best standards of protecting data in motion and at rest with encryption.

The access controls can help reduce the possibility of a data breach by having specifications of automatic logoff, encryption, and emergency access procedures according to (HIPAA Journal, 2018). Adding technical safeguards, the HIPAA compliance helps by having integrity control which makes sure there are no changes to the PHI (HIPAA Journal, 2018). Then there is person or entity authentication which makes sure that effective password policies are in place (HIPAA Journal, 2018). Also, HIPAA compliance has audit controls which make sure that the system has software to record event logs and examine activity for covered entities and business associates (HIPAA Journal, 2018). For implementing access controls for HIPAA compliance of technical safeguards you help your organization by minimizing a data breach. This is done by user identification and password management in your organization.

The security policies can help mitigate a data breach by having policies in place to respond to incidents. According to (NORCAL Risk Management, 2018) documentation of who is on the incident response team and what actions to take to address the incident. Also, use the HIPAA audit protocols to provide monitoring protocols (NORCAL Risk Management, 2018). Security policies for HIPAA compliance would be to analyze all sources, systems, movement, and storage of PHI. Document all the results of risk assessment and implement additional safeguards to correct any security risks identified (NORCAL Risk Management, 2018).

To comply with HIPAA compliance can help reduce the attack surface by mapping data flows which would include to or from Business Associates to simplify risk assessments and analyze and more efficiently identify threats to PHI according to (HIPAA Journal, 2018). Lastly, step nine on the HIPAA compliance list that says not to assume all users have the same level of knowledge and awareness (HIPAA Journal, 2018) as this can help you have better strategies and safeguards in place to reduce the attack surface to your organization.

Additional HIPAA IT (Information Technology) compliance can help the technology risk domain by updating existing security mechanisms according to (HIPAA Journal, 2018) an example of this would be to implement a legacy computer to the cloud and monitor user activity. If we did not change the existing security mechanisms, the legacy computer would not be able to go to the cloud due to the security risks found in the risk assessment. This way we can add the legacy computer to the cloud and have safeguards in place and use policies in place to protect it from attackers and not make this implementation a risk to the organization.

A multi-layered approach could be obtained by HIPAA compliance by password policies and mandatory MFA (multifactor authentication) (HIPAA Journal, 2018). Another HIPAA compliance is testing the incident response team and disaster recovery plans to ensure that all team members understand their role in such events according to (HIPAA Journal, 2018). Finally, reporting and monitoring should be automated to reduce the burden of user compliance and threat management (HIPAA Journal, 2018). This is a multi-layered approach because you are reducing administrative burdens on threat management and user compliance to give more time to respond to threats, testing disaster recovery plans and incident response plans to respond to threats effectively, and making the environment harder to breach by implementing password policies and mandatory MFA.

HIPAA compliance helps external contractors by having a business associate (BA) agreement. This helps by making sure under the Omnibus Rule the external contractor meets the independent responsibilities of Office of Civil Rights (OCR) to comply with HIPAA privacy, security, and breach notification rules (Stryker, 2017). If these are not followed the BA is fined by OCR according to (Stryker, 2017).

HIPAA compliance helps cloud-based solutions by controlling how the technology is used. HIPAA rules help to provide the account correctly and standard practices are applied (Alder, 2017). Also, to be HIPAA compliant according to (Alder, 2017) there must be two-factor authentication for access, make sure access-controls are configured correctly, use strong passwords, set the documents visibility to private, disable third-party apps and add-ons, and disable access to apps and add-ons. Also, audit access and account logs and share file reports regularly (Alder, 2017).

**References**

NORCAL Risk Management. (2018, June 4). *Preventing HIPAA Data Breaches: Case Studies and Best Practices*. Www.norcal-Group.com. <https://www.norcal-group.com/library/preventing-hipaa-data-breaches-case-studies-and-best-practices>

HIPAA Journal. (2018). *HIPAA Compliance Checklist*. HIPAA Journal. <https://www.hipaajournal.com/hipaa-compliance-checklist/>

Stryker, C. (2017, August 10). *Two Essentials for HIPAA Omnibus Final Rule Compliance | Physicians Practice*. Web.archive.org. <https://web.archive.org/web/20170810052932/https://www.physicianspractice.com/blog/two-essentials-hipaa-omnibus-final-rule-compliance>

Alder, S. (2017, July 21). *Is Google Drive HIPAA Compliant?* HIPAA Journal. <https://www.hipaajournal.com/is-google-drive-hipaa-compliant/>