Privacy laws are not sufficient to ensure that the sharing and use of data will meet the fair information practice principles of the organization because according to the HIPAA privacy rules Helios Health Insurance Inc must provide personal identifiable information with protection even if they are a business associate. The organization is not complying with HIPAA privacy rules as they are not saying they will protect their health information gained from customer's anonymous data. If this information is sent from fit vantage to Helios Health Insurance Inc the organization must comply with HIPPA privacy rules. Also, Helios Health Insurance Inc must say what they are using the information for from the customers as it is the customer's right to know what their information is used for by organizations (Health Information Privacy, 2019). Another privacy law is the Occupational Safety and Health Administration (OHSA) which requires covered entities to disclose information to public health authorities to collect information for preventing or controlling diseases, injury, or disability (HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, 2019). The organization Helios is not complying with the FISMA act as well because there is no security for information like encryption for receiving the anonymous information, multifactor authentication, and Helios does not say how they protect the customers password. Helios is failing to comply with the State Data Breach Notification Laws as they need to tell customers how they will contact them if there is a security breach that discloses their personal information in the future. Helios is failing also to comply with the documentation and recording retention as they need to maintain documentation for up to six years after the last effective date of their company. The privacy rule requires the company to document the company's policies and procedures, privacy practice notices, and arrangement of complaints. The organization is also not complying with COPPA as the customers are purchasing this fit-vantage flame through Helios. Customers need to have laws that protect their children’s privacy online and block age-inappropriate content.

Safeguards for control over customer's data would be minimum necessary for use and disclosure. Helios must try to request only the minimum amount of protected health information possible to do their job. Helios must make policies and standards for limiting access and use of protected health information. The customers should have the option of disclosures and use of their protected health information by giving their written authorization. Helios should tell customers certain situations when they will have to disclose protected health information like when it is required by law by statute, court order, or regulation. Helios should implement the reasonable reliance which states that if any covered entity makes a request for protected health information it must comply with the minimum necessary standard. A good safeguard is to shred documents that have protected health information before throwing them out (Rights (OCR), 2021). Another great safeguard is to make sure files are not easy to get to for an attacker. To do this a safeguard for Helios should be to protect customers' medical records with a lock and key (Rights (OCR), 2021). Lastly, Helios should only have a few people in their organization with access to these pass codes (Rights (OCR), 2021), usually people towards the top of the organization. These safeguards should be the minimum for customer's data use and disclosure.

My concerns for the Helios program are they do not have safeguards in place to protect sensitive information. Helios does not comply with many laws like state data breach notification law, HIPAA privacy rules, and FISMA. There is also another concern because they lack the ability to follow laws, there is nothing stopping Helios from gathering a bigger set of anonymous data from fit vantage. This data could come from fit vantage as Helios does not have any policies or procedures in place to even document that their anonymous information came from fit vantage without customers' approval. Without the documentation by Helios, it is almost impossible to hold them responsible for this as there is no trace of evidence. Fit vantage would be blamed for the HIPAA violation which would cost the company money and would cause conflict with their

core values. HIPAA transactions rule needs to be implemented so that Helios and fit vantage can share protected health information or identifiable information which is done by the standards of electronic data exchange (HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services, 2019). The company will lose customers but will gain two times the revenue. The likely effect on company stockholders is to partner with Helios because of the gain in revenue. Fit vantage customer base will lose half of its customers because of Helios as they are not comfortable sharing information with them, as 36.4% are not comfortable with sharing data anonymously. The core values of fit vantage do not align with this partnership as Helios is not complying with HIPAA laws and not telling customers what data they are anonymously collecting. The mission statement for fit vantage is to contribute to the health and well-being of every customer with technology that complements everyone's lifestyle, but this would not be the case because fit vantage would lose almost half of their customer base just from sharing data anonymously. Fit vantage should not partner with Helios because it will only hurt the customers of fit vantage and put fit vantage at risk of being sued because their partner was not good enough to comply with the laws and HIPAA privacy rules. Even if fit vantage did a business associates rule, fit-vantage would need a business associate contract that way fit-vantage can say what Helios Health Insurance Inc must protect to agree to the business associate agreement (Office for Civil Rights, 2008). This still does not work because their policies and standards, core values, and mission statement are much too different than fit vantage.

References

HIPAA Privacy Rule and Public Health Guidance from CDC and the U.S. Department of Health and Human Services*. (2019). https://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm

Health Information Privacy. (2019, January 4). Health Information Privacy. HHS.gov. https://www.hhs.gov/hipaa/index.html

Office for Civil Rights (OCR. (2008, May 21). Business Associate Contracts. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

Rights (OCR), O. for C. (2021, June 9). Health Information Privacy. HHS.gov. https://www.hhs.gov/ocr/hipaa/