**CYB 260 Project Two**

Douglas Few

Southern New Hampshire University

June 15, 2021

Data Privacy

In order to protect the privacy of customer data, we need to make sure we are only collecting data that is absolutely necessary. On top of this, it is imperative that we coordinate with both state and federal laws regarding data collection. Since every state has their own laws regarding consumer privacy, we need to make sure we are abiding by the laws of every state we plan to operate in. Most importantly, because our objective is to partner with a health organization to collect health information, we need to abide by the laws set forward in the Health Insurance Portability and Accounting Act (HIPAA). For example, according to the HIPAA privacy summary, any information that is “individually identifiable” is to remain confidential. This includes information regarding an individual’s past, present, or future health conditions (Secretary & (OCR), 2013).

Data Security

The security of personal data belonging to our customers is very important to keep in consideration, from an ethical and business perspective. In order to ensure the data security of our customers, I recommend we implement training programs for our employees that regularly focus on security awareness and avoiding scams that typically lead to information being leaked. The approach to ensuring data security that I would recommend would take form in two steps. The first step would be to develop a training regiment that is required for all employees that handle customer data. This training would occur in regular intervals, such as quarterly or bi-yearly, and would cover topics such as phishing scams and other social engineering topics to help raise employee awareness and educate on how to best counter these attacks. The second step would be to simulate phishing scams, send them to employees, and track their responses. This would not be in an attempt to punish or reprimand them, but rather to help them learn the importance of staying security-minded. This is, according to Dane Boyd with Aberdeen Research, the most effective way to conduct security awareness training (2017).

Ethical Considerations

As mentioned in previous memorandums written to the internal leadership board, I believe it is ethically irresponsible to continue moving forward with the implementation of this partnership. This is because a large percentage of our user base has stated they do not feel comfortable with sharing certain pieces of information regarding their health. It is for that reason that I believe we should be handling any information we do collect and share with our partnered organization with the utmost care. Doing so will allow Fit-vantage to remain acting ethically, as well as maximize profits by maximizing the amount of trust our consumers have in us as a business.

References

Boyd, D. (2017, August 24). *It's Time to Finally Kill "Traditional" Security Awareness Training*. Aberdeen Strategy & Research. https://www.aberdeen.com/techpro-essentials/time-finally-kill-traditional-security-awareness-training/.

Secretary, H. H. S. O. of the, & (OCR), O. for C. R. (2013, July 26). *Summary of the HIPAA Privacy Rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.