Southern New Hampshire University

CYB 260 Project One Milestone Template

Replace the bracketed text with the relevant information.

I. **Analysis of Requirements**

Select three fair information practice principles from the privacy statement provided by your instructor. Then fill in the cells in the table below.

Requirements Table

Fair Information Practice Principle	Applicable Privacy Law or Laws	Level of Compliance	Safeguards
Protecting Your Account	This principle aligns with the HIPAA Security Rule, which requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.	The organization meets the requirements as it stresses the importance of maintaining the confidentiality and integrity of user logon credentials, akin to the HIPAA Security Rule's requirements.	To ensure compliance, the company should implement two-factor authentication, regular password updates, and encrypted storage of credentials.
Personal Information and Choice	This principle is supported by the General Data Protection Regulation (GDPR), which grants individuals the right to access their personal information and the choice to consent to data processing.	The company exceeds GDPR requirements by not only allowing users to access and update their information but also by providing the option to opt-out of data collection.	Implement regular audits to ensure compliance and provide clear, accessible information on how users can manage their consent and personal information.

Fair Information Practice Principle	Applicable Privacy Law or Laws	Level of Compliance	Safeguards
Use of Cookies	This principle aligns with the ePrivacy Directive (Cookie Law), which mandates clear consent for the storage of or access to information on a user's device.	The company meets the requirements by informing users about the use of cookies and requiring consent before setting them.	The organization should ensure that cookie consent mechanisms are robust and clear and allow users easy options to withdraw consent at any time.

II. Business Implications

A. Discuss the role of ethics as a business driver in this decision. How do the organizational values (as an ethical stance) align with the decision? What responsibility does the organization have regarding privacy?

The organizational values of prioritizing good health and being good citizens align closely with the decision to enforce strict privacy policies. This ethical stance ensures that the company not only complies with legal standards but also upholds the trust and well-being of its users, which is fundamental to the organization's responsibility regarding privacy.

B. Discuss how your personal ethical stance aligns with the decision. How did you apply an ethical framework or decision strategy to inform your position?

My ethical stance, which values transparency and user empowerment in data handling, aligns with the company's decision. I applied the ethical framework of utilitarianism, aiming to produce the greatest good for the most significant number by supporting practices that enhance user trust and satisfaction.

C. What would you recommend the company do? Describe how you came to this decision. How did you balance differences between the organizational ethics and your own personal ethics?

I recommend that Fit-vantage continue to strengthen its privacy practices by integrating more user-friendly data management tools. This approach aligns with the organizational values of no fine print (transparency) and my personal ethics. It balances the business goal of user trust with sustainable growth.