Privacy Extended Response

Question 1

25 marks

A technology company is developing a new digital platform that integrates health and wellness services. Users sign up, provide extensive personal health data (e.g., medical history, fitness levels, dietary habits), and link their wearable devices to receive personalised health recommendations. The platform also intends to share aggregated, anonymised user data with research institutions.

a) Describe the critical considerations for the platform when collecting personal health information from users. Identify two Australian Privacy Principles that directly address the ethical and legal obligations of the platform in this collection process and explain how the platform should adhere to them. (9 marks)

b) Analyse the risks associated with the use, disclosure, and security of the sensitive personal health data collected by this platform. Identify two Australian Privacy Principles that are central to managing these risks and explain how the platform could implement measures to comply with these principles. (9 marks)

c) Discuss the concept of anonymity for users interacting with such a platform, considering its benefits and limitations. Evaluate the platform's decision to share "aggregated, anonymised" data with research institutions, weighing the value derived from this data against the ongoing challenges of protecting individual privacy. (7 marks)

Marking Guide

Part A

Marks	Criteria	Evidence of achievement
1	Identifies sensitive nature of health data	States health information is highly sensitive and requires strict protection.
1	Notes need for explicit user consent	Explains that informed consent is critical when collecting health data.
1	Mentions transparency in collection	Explains users must be told what data is collected and why.
1	Identifies APP 3 (Collection of solicited personal information)	States only necessary, relevant health data should be collected.
1	Explains APP 3 in context	Links to platform's obligation to justify and minimise data collection.
1	Identifies APP 5 (Notification of collection)	States users must be notified when and how data is collected.
1	Explains APP 5 in context	Example: clear privacy notices at signup outlining purpose of data use.
1	Provides concrete implementation	Suggests privacy policy, consent forms, or "just-in-time" notifications.
1	Integrates ethical and legal obligation	Links APPs to ethical duty to protect user autonomy and trust.

Sample Response

Collecting health information requires special care because medical history, fitness, and dietary data are highly sensitive. The platform must only collect information that is directly relevant to providing personalised recommendations and must obtain clear, informed consent from users. Transparency is critical so that users understand why their data is collected and how it will be used.

APP 3 (Collection of solicited personal information) requires that the company collect only what is necessary. For example, the platform should not ask for unrelated health conditions if they do not affect its service.

APP 5 (Notification of collection) requires the company to inform users about the collection, purpose, and intended uses of their health information. This can be achieved by displaying a clear privacy policy and providing just-in-time notices at signup. By following these principles, the platform aligns with both ethical and legal responsibilities.

Part B

Marks	Criteria	Evidence of achievement
1	Identifies risk of misuse	States personal health data could be misused for profit or insurance discrimination.
1	Identifies risk of unauthorised disclosure	States data leaks or sharing without consent could expose users.
1	Identifies risk of security breaches	Notes hacking or weak protection could expose sensitive health records.
1	Identifies APP 6 (Use or disclosure of personal information)	States data can only be used/disclosed for the purpose collected or with consent.
1	Explains APP 6 in context	Example: platform cannot sell identifiable health data to third parties.
1	Identifies APP 11 (Security of personal information)	States reasonable steps must be taken to secure personal data.
1	Explains APP 11 in context	Example: data encryption, strict access controls, regular audits.
1	Provides concrete security measure	Example: end-to-end encryption of wearable device data.
1	Integrates risk analysis with APPs	Links threats directly to compliance obligations and mitigation strategies.

Sample Response

Sensitive health data carries significant risks. If misused, it could be exploited for targeted advertising or insurance discrimination. If disclosed without consent, it could undermine user trust and expose private conditions. If security is weak, breaches could release medical records into the public domain.

APP 6 (Use or disclosure of personal information) requires that data be used only for the purpose it was collected, unless users give explicit consent. For example, the platform cannot sell identifiable health data to third parties for marketing.

APP 11 (Security of personal information) requires organisations to take reasonable steps to protect personal data. Implementation measures include strong database encryption, secure transmission from wearable devices, role-based access control for employees, and regular security audits. By applying these safeguards, the platform reduces misuse, limits disclosure, and upholds its duty to protect user data.

Part C

Marks	Criteria	Evidence of achievement
1	Defines anonymity	States anonymity means individuals cannot be identified from their data.
1	Explains benefit of anonymity	Example: reduces privacy risks and increases user trust.
1	Explains limitation of anonymity	Example: risk of re-identification when data sets are combined.
1	Evaluates aggregated anonymised data	States it allows valuable insights for research without exposing individuals directly.
1	Explains data value in health research	Example: helps discover public health trends and improve treatments.
1	Identifies privacy challenge	Notes anonymisation is not foolproof, requiring ongoing safeguards.
1	Balances value vs privacy	Concludes sharing is useful but must be paired with safeguards to protect identities.

Sample Response

Anonymity allows users to engage with the platform without their identity being revealed in datasets. This provides a benefit by reducing privacy risks and encouraging participation. However, anonymity has limitations because re-identification can occur if anonymised data is combined with other datasets.

The decision to share aggregated, anonymised data with research institutions has value. It enables public health researchers to identify trends, improve treatments, and support evidence-based policy without accessing individual records. This data is particularly useful for understanding population-level health issues.

The challenge lies in ensuring that anonymisation techniques remain strong. Even aggregated data must be carefully managed to prevent re-identification. Therefore, the platform's approach balances value and privacy: sharing data contributes to research but requires ongoing safeguards, such as de-identification standards and regular privacy reviews.