Congratulations! You passed!

Grade received 100% **To pass** 80% or higher

Go to next item

GDPR and Privacy

Total points 4

1. How actual users experience your system is essential for assessing the true impact of its predictions, recommendations, and decisions. A straightforward technique to incorporate that feedback is using several metrics rather than a single one. What types of metrics can help you understand tradeoffs between errors and experiences? (Select all that apply) **1 / 1 point**

- [x] Short and long-term product health measures

  Correct
  You've got it! These measures include click-through rate and customer lifetime value, respectively.

- [x] False-positive and false-negative rates

  Correct
  Right on track! We calculate classification metrics such as accuracy, precision, recall, and F1-score based on these rates.

- [x] Overall system performance metrics

  Correct
  Keep it up! Using different metrics for performance evaluation improves the overall predictive power of our model before we roll it out for production. Depending only on accuracy can lead to poor predictions on unseen data.

- [x] User surveys

  Correct
  Great job! Engaging with diverse users and different use-case scenarios will build a wide variety of perspectives into the project and benefit as many people as possible.

- [ ] Automated quality characteristics measures

2. True or False: Informational harm occurs when the adversary is able to inject bad data into your model's training pool. This attack is known as poisoning. **1 / 1 point**

- (•) False
- ( ) True

  Correct
  You're right! We are describing behavioral harm, as the attack aims to inject so much bad data into your system that whatever boundary the model learns becomes useless.

3. How can a hospital network that wants to improve its models and predictions collaborate without sharing information directly between institutions and violating healthcare privacy laws? **1 / 1 point**

- ( ) Using Differentially-Private Stochastic Gradient Descent.
- ( ) Using Trusted Execution Environments.
- (•) Using Confidential and Private Collaborative Learning.
- ( ) Using Cryptography.

  Correct
  Exactly! CaPC Learning enables multiple developers with different data to collaborate and improve their model accuracy without sharing information. To preserve both privacy and confidentiality, CaPC leverages secure multi-party computation (MPC), homomorphic encryption (HE), and other techniques in combination with privately aggregated teacher models.

4. Does pseudonymized data cease to be "personal data" and stop requiring compliance with the GDPR? **1 / 1 point**

- ( ) Yes, because pseudonymization irreversibly prevents identifying the individual to whom the data relates using masking, encryption, or tokenization.
- (•) No, because pseudonymization is a reversible process, meaning it's still possible to identify the individual if the correct additional information or encryption key is included.

  Correct
  Absolutely! Pseudonymized data remains "personal data" as it still can be attributed to a specific data subject using additional information kept separately. Moreover, even where effective anonymization takes place, other regulations may apply.