## Candidate Assessment Quiz

### Computation over encrypted data using the TFHE (Fast Fully Homomorphic Encryption over the Torus) library.

Fully Homomorphic Encryption schemes allow arbitrary computation on encrypted data. These computations are carried in form of Boolean circuits. FHE schemes, however, also add noise to the ciphertexts, and the noise increase with evaluation of every logic gate. Hence, after certain number of computations, it becomes impossible to decrypt the ciphertexts correctly. Bootstrapping is the process through which noise can be reduced from the ciphertexts.

TFHE library has been developed to fasten the bootstrapping process, and hence improve efficiency of the overall computation.

### Assessment task:

Utilize TFHE to implement the following:

- Question 1: Add all TotalCharges values where CCS Diagnosis Code = 122
- Question 2: Count number of even values in TotalCharges.
- Question 3: Count number of TotalCost>10000.
- Question 4: Parallelize Question 3 using multi threading.

After implementation, provide your assessment on the following aspects:

a. Is there a limit on the number of TotalCharges values, which can be added correctly using the library?
b. Running time for addition (a).
c. How much does the ciphertext increase in length as compared to the plaintext value?

Supporting material:

The TFHE library is available at https://github.com/tfhe/tfhe .

Tutorial for the library is available at https://tfhe.github.io/tfhe/ . Please feel free to utilize the examples and test scripts provided in tutorial and source code for implementation of tasks (a) and (b).

Understanding of the mathematical concepts behind the encryption scheme is not required for the assessment.