

Secure Aggregation

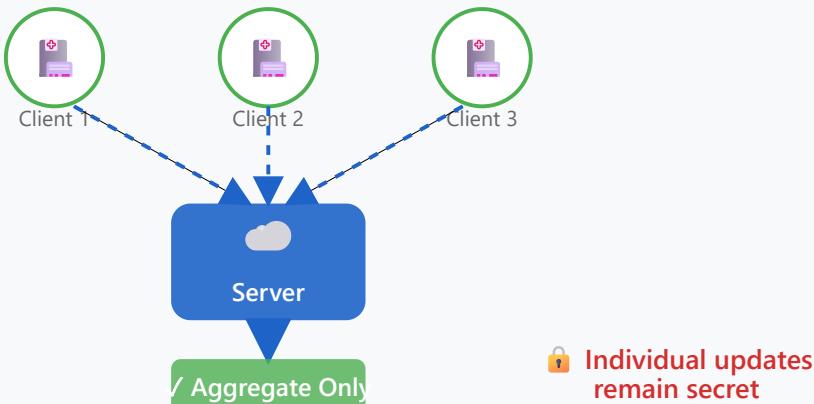
Server learns only aggregate, not individual updates

Process

1 Clients mask updates
 $u_1 + m_1 = w_1$ masked

2 Server aggregates
 $m_1 + m_2 + m_3 = \Sigma(\text{masked})$

3 Masks cancel in sum
 $m_1 + m_2 + m_3 = Q$



Shamir Secret Sharing

Split secrets into shares

Homomorphic Encryption

Compute on encrypted data

Secure Multi-Party Computation

Joint computation without revealing