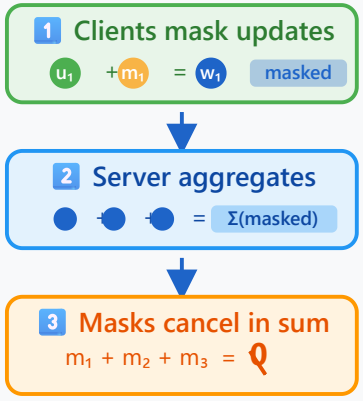
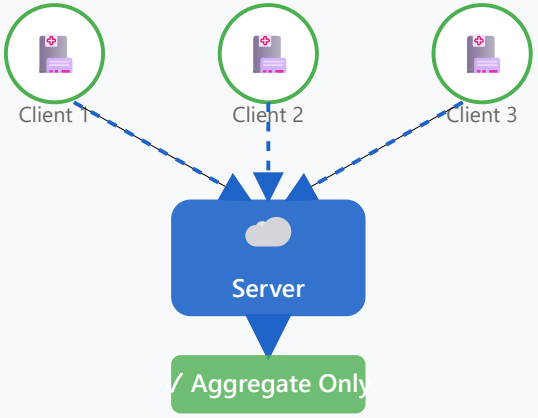
Secure Aggregation

Server learns only aggregate, not individual updates

Process





Individual updates remain secret

Shamir Secret Sharing
Split secrets into shares

Homomorphic Encryption
Compute on encrypted data

Secure Multi-Party Computation
Joint computation without revealing