Differential Privacy (Weaker Notion)

X: The data *universe*.

$D \subset X$: The dataset (one element per person)

Definition: An algorithm M is $(\boldsymbol{\epsilon}, \boldsymbol{\delta})$**-differentially private** if for all pairs of neighboring datasets D, D', and for all outputs x:

$$\Pr[M(D) = x] \leq \exp(\boldsymbol{\epsilon}) * \Pr[M(D') = x] + \boldsymbol{\delta}$$

Quantifies information leakage **Allows for a small probability of failure**

Some useful properties for ML

- **Theorem** (**Post-processing**): If $M(D)$ is ϵ-private, and f is any function, then $f(M(D))$ is ϵ-private.

- **Theorem** (**Composition**): If $M_1, \ldots, M_k$ are ϵ-private, then

$M(D) \equiv \left(M_1(D), \ldots, M_k(D)\right)$ is $(k * \epsilon)$-private.

- We can design algorithms as we normally would. Just access the data using differentially private **subroutines**, and keep track of our "privacy budget" (**modularity**)