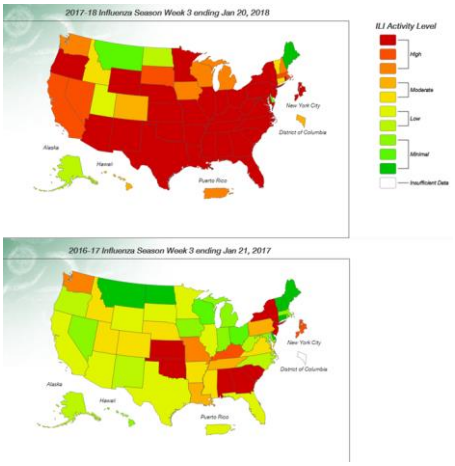
Implemented by DRIVENDATA hero^x Hosted by NIST PSCR PUBLIC SAFETY COMMUNICATIONS RESEARCH

Differential Privacy Temporal Map Challenge

Help public safety agencies share data while protecting privacy.



Sample temporal map data on flu activity in Jan. 2017 and 2018 (Source: CDC FluView)

Large data sets containing personally identifiable information (PII) are exceptionally valuable resources for research and policy analysis in a host of fields supporting America's First Responders such as emergency planning and epidemiology.

Temporal map data—information that is geographically situated and may change over time—is of particular interest to the public safety community in applications such as optimizing response time and personnel placement, natural disaster response, epidemic tracking, demographic data and civic planning. Yet, the ability to track a person's location over a period of time presents particularly serious privacy concerns.

The Differential Privacy Temporal Map Challenge will invite solvers to **develop algorithms and metrics that preserve data utility while guaranteeing individual privacy is protected**.

Participants compete in a series of coding sprints using differential privacy methods on temporal map data. These data sets may contain the records of hundreds or thousands of individuals, each contributing to a sequence of events. The goal is to create a privacy-preserving dashboard map that shows changes across different map segments over time.

Top solutions will be publicly recognized and up to **$276,000 in cash prizes** may be awarded to best-performing teams.

The NIST PSCR Differential Privacy Temporal Map Challenge follows on the success of the 2018 Differential Privacy Synthetic Data Challenge, extending the reach and utility of differential privacy algorithms.

- **Temporal map data**: The challenge will feature public safety data sets with geographic and temporal elements. Solutions will seek to satisfy differential privacy while preserving characteristics of original data sets as much as possible, including sequential data and geographic characteristics.
- **Utility metrics**: Participants may submit white papers on new and innovative ways of measuring the accuracy of data sets produced by differential privacy algorithms.
- **De-identification algorithms**: Participants build and submit algorithms to preserve data accuracy while guaranteeing privacy on temporal map data sets.
- **Open source development**: Beyond expanding the types of data that can be made differentially private, this challenge seeks to advance and disseminate the resulting software.

Learn more and sign up for challenge updates at **deid.drivendata.org**.