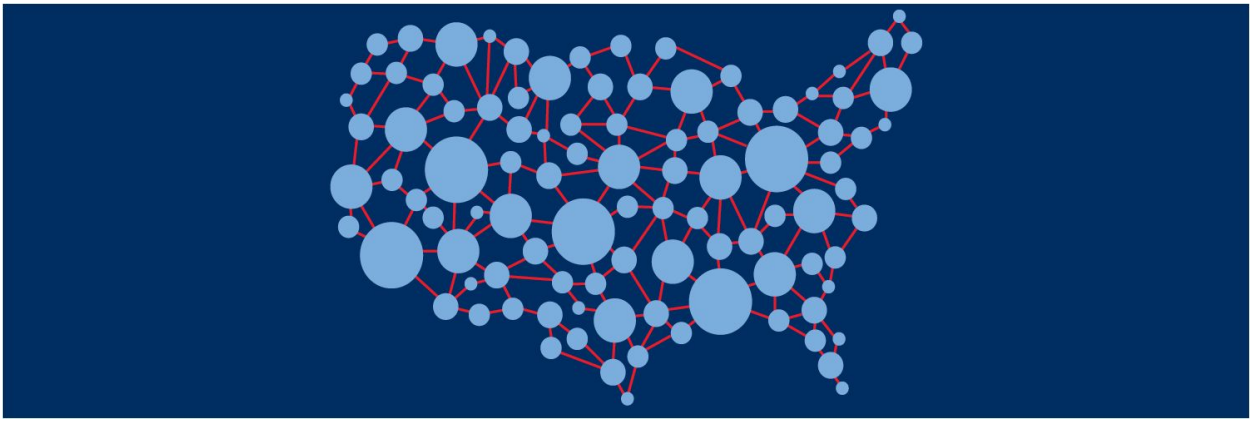
April 30, 2020

7 Ways to Boost Data Impact in Response to the Pandemic: Advice from the Nation's State Chief Data Officers



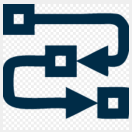
The COVID-19 pandemic is affecting every state and illuminates the critical role data plays in their response efforts. The members of the State Chief Data Officers Network, which consists of 25 state Chief Data Officers across the country, are stepping up to support their states' efforts to use data. Whether understanding supplies of personal protective equipment, which hospitals are nearing capacity, or reporting accurate testing data to the public, state CDOs are leaning in to improve how data are shared and used.

Based on CDOs experiences to date, adopting effective practices in the COVID-19 response will help states move from crisis to recovery. Right now states are focused on sharing data about testing, infection rates in nursing homes and correctional facilities, and unemployment. In the future, state leaders will need the right data to inform the recovery phase and how to best reopen child care centers, economic sectors, and schools.

The following are best practices the State Chief Data Officers Network recommends to improve states' ability to share and use data during this crisis and through recovery.

Coordinate data management

Establish an interagency data coordinating body, ideally led by the Chief Data Officer. A data coordinating body should be part of the state response framework or incident command structure. This allows the data experts to communicate and coordinate directly with response on various data needs and issues. If a state doesn't have a formal CDO role, appoint one. The State Chief Data Officers Network has crafted guidance for states on establishing a CDO role and has compiled a selection of job descriptions states can use. The State CDO's role should include facilitating data sharing between municipal, county and tribal governments within the state.



Remove barriers to data sharing

Create streamlined and transparent legal processes necessary for data sharing. Several states already have "enterprise" data sharing memorandums of agreement that lay the basic legal foundation for the sharing of data. These global agreements are supported by specific, templated, business or use case documents for individual instances of data sharing. This prevents the need to negotiate and re-negotiate terms for each data sharing need.

a. Prior to initiating any form of data sharing agreement, parties should be clear about: who will see the data, how it will be accessed, how it will be used, for how long, how it will be protected, and what happens after the agreement ends.
b. In instances where a legal opinion precludes the sharing of data, these opinions should be formally documented and explain the legal reasoning why data cannot be shared so that parties have an opportunity to resolve any conflicts.

Arizona and California are leveraging enterprise memorandums of agreement and standard data sharing agreements to speed the exchange of data.

Make data discoverable

Even when data is protected, the information about what data each agency has generally is not. By making information such as metadata and data dictionaries available through a centralized repository, states will have a better understanding of what exists and how it can be used.

> *Virginia recently released a publicly available metadata catalog detailing the data holdings of many of its agencies.*

Format data to be useful

Ensure any data exchanged is in a machine-readable format (searchable, sortable, and digital) at the finest level of granularity allowed by law that's necessary given the intended use. When sharing data internally within the government, it should be aggregated or use suppression of small values consistent with the minimum access necessary to complete the intended use.

Centralize data access across agencies

Data that can be shared within government should be accessible through a centralized clearinghouse or repository. These should be accompanied by robust security and privacy controls to ensure that individuals can only access data for which they are authorized users. Data in central repositories should be managed and governed so that users are assured that it is fit for its intended use.

> *Indiana and North Carolina leverage statewide data warehouses that can readily accept and secure new sources of data and make them available to appropriate individuals for analysis.*

Publish public data as open data

When data is public, make sure it's available through the state's open data website. If a state doesn't currently have an open data website, establish a webpage and provide datasets in open non-proprietary formats such as comma separated values (csv). While PDFs and Dashboards are great for communicating top-level findings, they should always be accompanied by machine-readable open data.

> *Connecticut, New Jersey, and New York are publishing COVID-19 and other related datasets on their open data portals.*

Lead with the analysis

Not everyone is comfortable with or has the time to work with raw data. State leaders and the public often need easily digestible information at their fingertips. Readily available reports and dashboards can help people answer questions quickly.

> *Maryland's COVID-19 website provides easy access to top level statistics.*

Chief Data Officers can play a critical role in supporting emergencies like COVID-19 by using their centralized position to get the right data to the right people in a timely fashion. As state governments adjust to remote work, these practices will improve the way agencies communicate about and use data.