April 2021
OIG File #20-1263

Why We Conducted This Audit

Contact tracing—the process of identifying individuals with an infectious disease and alerting others who may have been exposed—is key to slowing the spread of COVID-19. If people are not confident their personal information will be secure, they are less likely to cooperate with contact tracers. We sought to determine if CDPH mitigates privacy and security risks associated with collection, storage, and transmittal of COVID-19 contact tracing data in accordance with City policies and CDC guidance.

Background

CDPH has taken a community-based approach to COVID-19 contact tracing, employing community-based organizations and their staff to lead the effort.

CDPH developed CARES to help contact tracers gather, organize, and store information so the Department can provide support to persons diagnosed with the disease and interrupt the spread of the virus by notifying close contacts.

We thank CDPH staff and management for their cooperation during the audit.

AUDIT OF CDPH COVID-19 CONTACT TRACING PROGRAM: DATA PRIVACY AND CYBERSECURITY

OIG found that the Chicago Department of Public Health (CDPH) COVID-19 contact tracing program mitigates data privacy and cybersecurity risks. Although certain improvements to policies and procedures would encourage consistent and timely application of the security measures, the Department's efforts to safeguard data suggest that the public's personal information will be protected.

Finding

CARES—CDPH's electronic case management tool—meets the cybersecurity and access control requirements of the City's Information Security and Technology Policies (ISTP). Contact tracer training aligns with the ISTP and includes several elements to develop data privacy awareness and information security principles. These training materials and procedures are stored within Microsoft Teams for easy access by contact tracers. CDPH has policies to mitigate risks when exchanging confidential information through electronic communication and to designate persons responsible for reviewing data requests. Contact tracers inform patients that their information will remain confidential and secure and obtain consent before proceeding. However, they do not tell patients and contacts how long CDPH will retain their information. Finally, CDPH did not consistently remove access to CARES for terminated users within seven days, in accordance with the ISTP.

Recommendations

OIG recommends that CDPH adjust its process for removing access to CARES for terminated users to ensure it is completed within seven days of termination. CDPH should also update the contact tracers' call script to inform patients and contacts how long the City will retain their data. Finally, the Department should update its data release policy to include explicit criteria for staff to reference in determining whether to grant data requests.

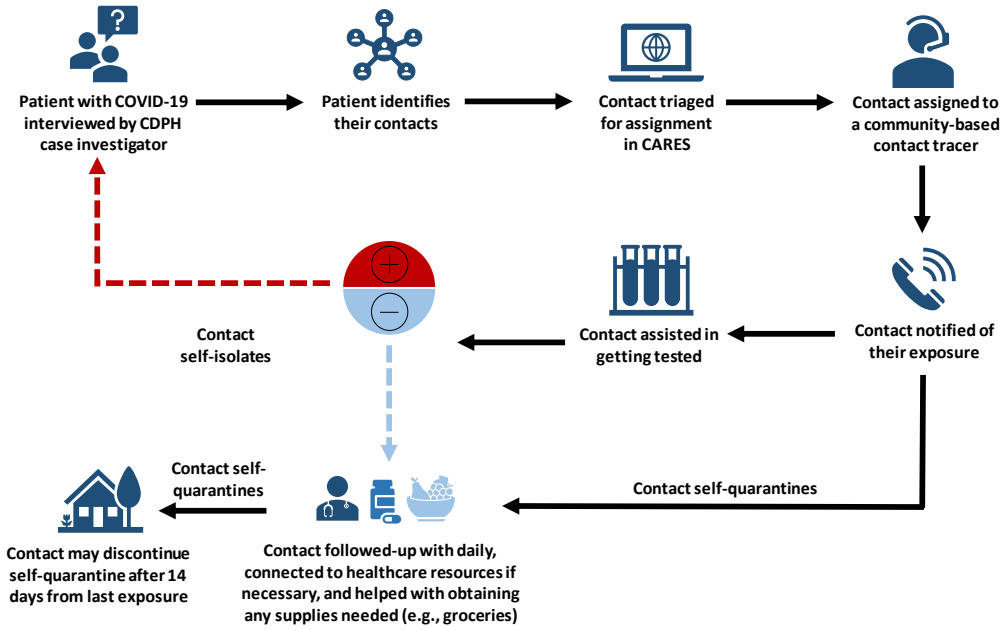
Department Response

In response, CDPH stated that it will incorporate employment status reviews into its weekly check-ins with the Chicago Cook Workforce Partnership and community-based organizations that employ the contact tracers, which the Department believes will allow it to promptly remove access to the system for terminated employees. The Department also stated that it will create a data retention policy for CARES and will update the call script so that staff inform interviewees how long their data will be retained. Finally, CDPH stated that it will create criteria to help guide staff when reviewing data requests.

April 2021
OIG File #20-1263

AUDIT OF CDPH COVID-19 CONTACT TRACING PROGRAM: DATA PRIVACY AND CYBERSECURITY (CONTINUED)

Chicago COVID-19 Contact Tracing Process



Source: OIG visual created from information on City of Chicago webpage.