APRIL 2021

AUDIT OF THE CHICAGO DEPARTMENT OF PUBLIC HEALTH COVID-19 CONTACT TRACING PROGRAM: DATA PRIVACY AND CYBERSECURITY

CITY OF CHICAGO
OFFICE OF INSPECTOR GENERAL

JOSEPH M. FERGUSON
INSPECTOR GENERAL FOR THE CITY OF CHICAGO

LISE VALENTINE
DEPUTY INSPECTOR GENERAL FOR AUDIT & PROGRAM REVIEW

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 4
A. CONCLUSION 4
B. FINDING 4
C. RECOMMENDATIONS 4
D. CDPH RESPONSE 5
II. BACKGROUND 6
A. CONTACT TRACING 6
B. CHICAGO COVID-19 CONTACT TRACING 7
C. CARES ELECTRONIC CASE MANAGEMENT TOOL 9
D. CITY OF CHICAGO INFORMATION SECURITY AND TECHNOLOGY POLICIES 9
E. CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC) CONTACT TRACING GUIDANCE 9
1. Standards to Facilitate Data Sharing and Use of Surveillance Data for Public Health Action 9
2. Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing 10
III. FINDING AND RECOMMENDATIONS 11
FINDING: CDPH'S COVID-19 CONTACT TRACING PROGRAM MITIGATES DATA PRIVACY AND CYBERSECURITY RISKS. 11
1. CARES meets the security requirements of the City's Information Security and Technology Policies 11
2. CARES access controls meet the security requirements of the City's Information Security and Technology Policies, but CDPH did not promptly remove access for all terminated users 12
3. Training for contact tracers aligns with the City's Information Security and Technology Policies, and CDPH maintains a record of all contact tracers' completion of training 13
4. CARES prompts contact tracers to inform individuals that all information will be confidential and secure, and requires individuals' consent to be recorded, but does not prompt notification of how long the City will store the information 13
5. CDPH has policies to mitigate risks when exchanging confidential information through electronic communications 14
6. CDPH has policies that designate persons responsible for reviewing data requests, but does not provide explicit criteria for determining whether to release data 14
IV. OBJECTIVE, SCOPE, AND METHODOLOGY 16
A. OBJECTIVE 16
B. SCOPE 16
C. METHODOLOGY 16
D. STANDARDS 17
E. AUTHORITY AND ROLE 17

ACRONYMS

AIS	Department of Assets, Information and Services
CARES	COVID-19 Assessment and Response Electronic System
CBO	Community-Based Organization
CDC	United States Centers for Disease Control and Prevention
CDPH	Chicago Department of Public Health
FedRAMP	Federal Risk and Authorization Management Program
HIPAA	Health Insurance Portability and Accountability Act
HITRUST	Health Information Trust Alliance
ISO	Information Security Office
ISTP	City of Chicago Information Security and Technology Policies
OIG	Office of Inspector General
PHI	Protected Health Information
PII	Personally Identifiable Information

City of Chicago
Office of Inspector General

AUDIT OF THE CHICAGO DEPARTMENT OF PUBLIC HEALTH (CDPH) COVID-19 CONTACT TRACING PROGRAM DATA PRIVACY AND CYBERSECURITY

CARES, CDPH's electronic case management tool:

- Meets requirements of the City's Information Security and Technology Policies (ISTP)
- Is certified by FedRAMP and HITRUST
- Includes a suite of security features to keep contact tracing data secure: active threat monitoring, data encryption, user activity reports, and audit trails
- Includes controls, such as role-based access and multi-factor authentication, to mitigate the risk of improper access

CDPH did not promptly remove system access for all terminated users: 26% of terminated users still had access to CARES at least a month after termination. CDPH provided a user activity report demonstrating that none of these individuals logged in to CARES after their employment ended.

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) conducted an audit of the data privacy and cybersecurity of the Chicago Department of Public Health's (CDPH) COVID-19 contact tracing program. Contact tracing is a disease control strategy that involves identifying persons diagnosed with COVID-19 and their contacts, then working with these individuals to stop further transmission. CDPH developed an electronic case management tool to support the work of its COVID-19 contact tracing teams. The COVID-19 Assessment and Response Electronic System (CARES) is a cloud-based data system that allows contact tracers to 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 their close contacts .

The objective of the audit was to determine if CDPH managed privacy and cybersecurity risks associated with the collection, storage, and transmittal of COVID-19 contact tracing data in accordance with the City of Chicago's Information Security and Technology Policies (ISTP) and the United States Centers for Disease Control and Prevention (CDC) guidance.

A. CONCLUSION

OIG concluded that CDPH's 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.

B. FINDING

OIG found that the electronic case management tool, CARES, meets the cybersecurity and access control requirements of the City's ISTP. However, CDPH did not consistently remove terminated users' access to CARES within seven days, in accordance with ISTP timeliness standards. We found that training for contact tracers aligns with the City's ISTP and includes several elements to develop awareness of data privacy and information security principles. We also found that contact tracers notify patients and contacts that their information will remain confidential and secure, and obtain consent before proceeding. However, contact tracers do not tell patients and contacts how long the City will retain their information. CDPH also has policies to mitigate risks when exchanging confidential information through electronic communication, and policies to designate persons responsible for approving data requests.

C. RECOMMENDATIONS

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

D. CDPH RESPONSE

In response to our audit finding and recommendations, 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.

The specific recommendations related to the finding, and CDPH's response, are described in the "Finding and Recommendations" section of this report.

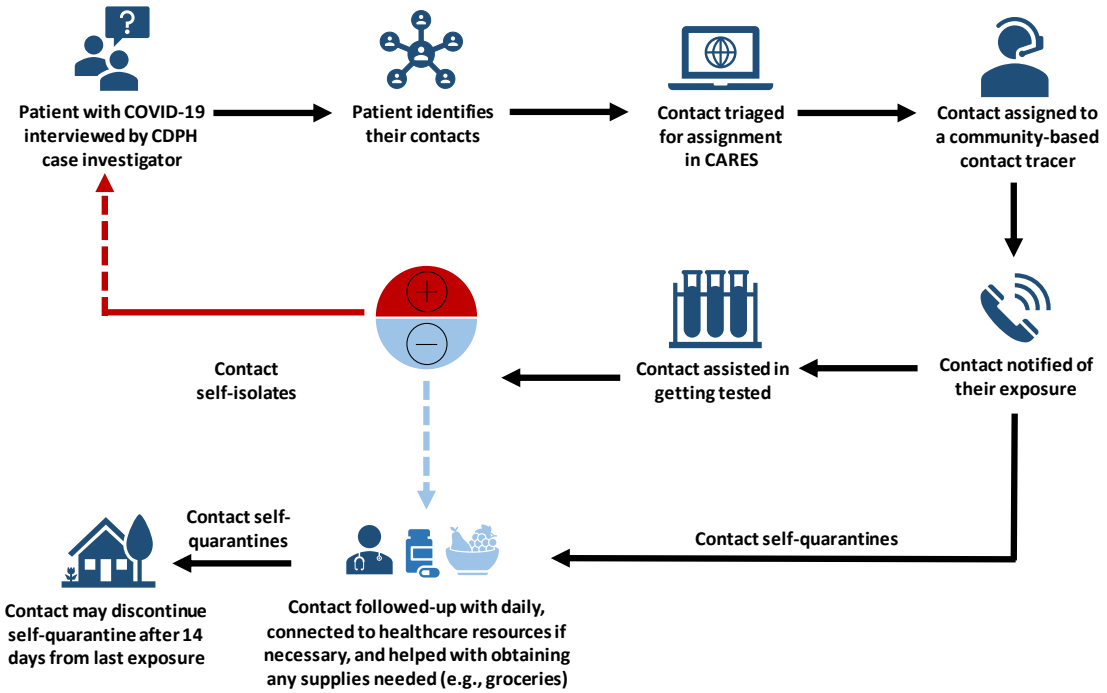
II. BACKGROUND

A. CONTACT TRACING

Contact tracing is a disease control strategy that involves identifying persons diagnosed with a disease and their contacts, then working with these individuals to interrupt further transmission. Local and state health departments have employed this strategy for decades. Contact tracing is key to slowing the spread of disease by letting people know that they may have been exposed and providing them with information on how to monitor their health for symptoms. It also helps these individuals get tested and connects them to resources and support during their time of self-isolation (if they have the disease) or self-quarantine (if they had close contact with someone who has been infected).

As illustrated in Figure 1, the City's COVID-19 contact tracing process begins when a case investigator reaches out to a person recently diagnosed with the disease. The investigator inquires about the person's symptoms, and asks where they have spent time and may have exposed others to COVID-19. Contact tracers then reach out to people who have been near the positively diagnosed person to notify them of their exposure and ask them to quarantine. Contact tracers also help these individuals get tested and connect them to support services. Contact tracers follow up with the contacts to check on symptoms and provide help as needed.

FIGURE 1: Chicago COVID-19 contact tracing process



Source: OIG visual created from information on City of Chicago webpage.[1]

[1] City of Chicago, COVID Contact Tracing Corps, "What is Contact Tracing," accessed February 3, 2021, https://www.chicago.gov/city/en/sites/covid-19/home/contact-tracing.html.

According to the United States Centers for Disease Control and Prevention (CDC), engagement with community members is a vital component of contact tracing programs.[2] CDC recommends that key public officials engage with communities to create a supportive environment for such efforts. A successful contact tracing program requires public awareness, understanding, and acceptance of the process, as well as willingness on the part of contacted individuals to separate themselves from others who have not been exposed.

A Pew Research Center survey on contact tracing conducted in July 2020 found that some Americans feel uncomfortable engaging with contact tracing programs.[3] For example, 41% of respondents said they would be "not at all" or "not too likely" to speak with a public health official contacting them about COVID-19. The survey found that 68% of Americans believe their personal information is less secure than it used to be. Additionally, the survey found that 41% of respondents said they are "not at all" or "not too" confident in public health organizations' ability to protect their personal records from unauthorized users.

B. CHICAGO COVID-19 CONTACT TRACING

Since its inception, the Chicago Department of Public Health (CDPH) has regularly engaged in contact tracing. CDPH's Case Investigations group has used contact tracing for other infectious conditions, such as measles and sexually transmitted diseases. At the onset of the COVID-19 outbreak in Chicago, CDPH's Case Investigations group led contact tracing efforts. As the disease quickly spread, the group became overwhelmed and the City determined it needed to expand its contact tracing operation.

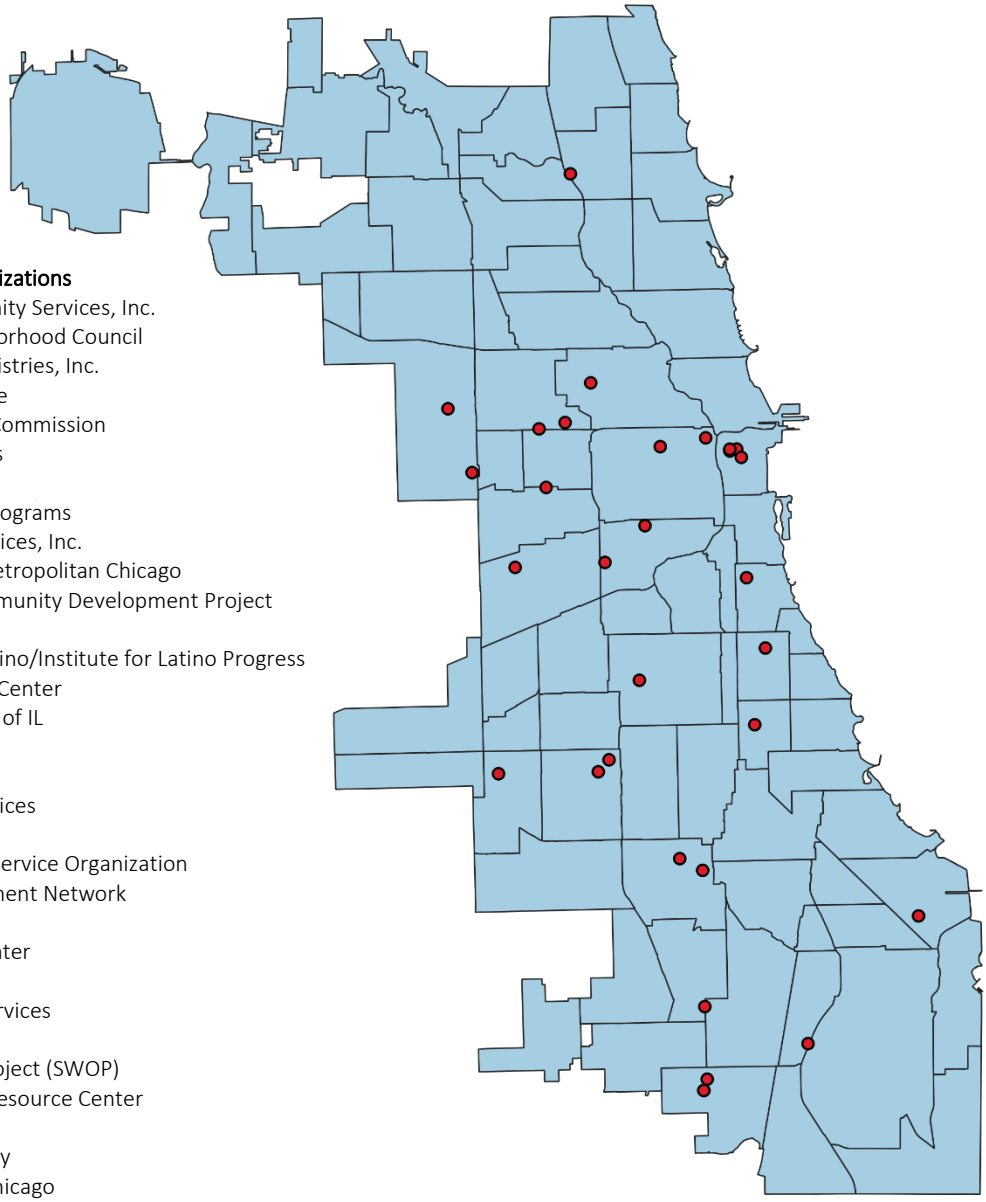
In May of 2020, the City issued a $56 million request for proposals to expand contact tracing efforts. The City selected the Chicago Cook Workforce Partnership, in collaboration with the University of Illinois at Chicago School of Public Health, National Opinion Research Center at the University of Chicago, Malcolm X College, and Sinai Urban Health Institute, to lead the effort of training and certifying a COVID-19 contact tracing workforce. Thirty-one community-based organizations (CBOs) in areas of high economic hardship received sub-grants from the Partnership to train and certify a 600-person workforce to support contact tracing and resource coordination. As of December 2020, CBOs had hired 589 contact tracers, 336 of which had completed their training.

Under the City's community-focused approach to COVID-19 contact tracing, there is an emphasis on building community trust and promoting equity. Because CBOs work and are familiar with community members, CDPH leadership believes that residents may feel more comfortable communicating with contact tracers employed by those organizations. Additionally, the City's

[2] Centers for Disease Control and Prevention, "Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic," 2020, accessed February 3, 2021, https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.
[3] Pew Research Center, "The Challenges of Contact Tracing as U.S. Battles COVID-19," 2020, accessed February 3, 2021, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/10/PI_2020.10.30_contact-tracing_REPORT.pdf.

approach aims to build public health skillsets in some of Chicago's most disadvantaged communities by funding CBOs and training their staff. Figure 2 provides the names and locations of CBOs engaged in contact tracing throughout the city.

FIGURE 2: Community-based organizations participating in COVID-19 contact tracing



Community-Based Organizations
Ada S. McKinley Community Services, Inc.
Back of the Yards Neighborhood Council
Breakthrough Urban Ministries, Inc.
Brothers Health Collective
Calumet Area Industrial Commission
Centers for New Horizons
Central States SER
Community Assistance Programs
Envision Community Services, Inc.
Goodwill Industries of Metropolitan Chicago
Greater West Town Community Development Project
Habilitative Systems, Inc.
Instituto del Progreso Latino/Institute for Latino Progress
KLEO Community Family Center
Latino Resource Institute of IL
Lawrence Hall
Leave No Veteran Behind
Metropolitan Family Services
National Able Network
New Pisgah Community Service Organization
North Lawndale Employment Network
Phalanx Family Services
Puerto Rican Cultural Center
Safer Foundation
SGA Youth and Family Services
South Side Help Center
Southwest Organizing Project (SWOP)
St. Sabina Employment Resource Center
The Resurrection Project
Westside Health Authority
YWCA of Metropolitan Chicago

Source: OIG visual created from information on City of Chicago web page.[4]

[4] City of Chicago, COVID Contact Tracing Corps, "Selected Community Based Organizations," accessed February 3, 2021, https://www.chicago.gov/city/en/sites/covid-19/home/chicago-covid-contact-tracing-corps.html.

C. CARES ELECTRONIC CASE MANAGEMENT TOOL

In late Spring 2020, CDPH began working with Salesforce, a cloud computing service company, to create the COVID-19 Assessment and Response Electronic System (CARES), a new electronic case management tool for contact tracing. CDPH stated that it chose the Salesforce platform because it has a secure data environment the Department can use for storing COVID-19 contact tracing data. CARES uses the Salesforce Shield and Salesforce Government Cloud products. Salesforce describes Shield as a service that provides enhanced protection, monitoring, and retention of data, and Government Cloud as a service only available to government entities and designed to address their specific security requirements. These products are certified by the Health Information Trust Alliance (HITRUST) and the Federal Risk and Authorization Management Program (FedRAMP).[5]

CARES also utilizes a multi-factor authentication login service provided by Okta, an internet identity company. Multi-factor authentication provides an additional layer of login security to help ensure that even if a user's password is compromised, their account remains protected.

D. CITY OF CHICAGO INFORMATION SECURITY AND TECHNOLOGY POLICIES

In the development of CARES, CDPH worked with the Department of Assets, Information and Services (AIS) to ensure that the software complied with the City's Information Security and Technology Policies (ISTP). The ISTP prescribe the minimum technology security requirements for City departments. These policies were developed based on two industry frameworks: National Institute of Standards and Technology, and International Organization for Standardization. AIS included additional requirements in the ISTP to comply with Payment Card Industry standards, the federal Health Insurance Portability and Accountability Act (HIPAA), and the Illinois Local Records Act.

E. CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC) CONTACT TRACING GUIDANCE

CDC has issued multiple guidance documents related to the COVID-19 pandemic, including two on safeguarding personal information when engaged in contact tracing.

1. Standards to Facilitate Data Sharing and Use of Surveillance Data for Public Health Action[6]

[5] HITRUST certification enables vendors and covered entities to demonstrate compliance with HIPAA requirements. FedRAMP is a compliance program established by the U.S. government that sets a baseline for cloud products and services regarding authorization, security assessment, and continuous monitoring.
[6] Centers for Disease Control and Prevention, "Standards to Facilitate Data Sharing and Use of Surveillance Data for Public Health Action," March 5, 2014, accessed February 3, 2021, https://www.cdc.gov/nchhstp/programintegration/sc-standards.htm.

CDC developed these standards based on ten guiding principles for data collection, storage, sharing and use.[7] They include recommended standards to ensure the security, confidentiality, and appropriate use (to include sharing) of data collected by contact tracing programs.

2. Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing[8]

CDC has also issued guidelines regarding two general aspects of the use of digital tools for contact tracing—first, timeliness and efficiency in the contact tracing process, and second, the minimum and preferred features of such resources. These guidelines are based on research and ongoing discussions with contact tracing and informatics experts across local, state, territorial, tribal, and federal government agencies; national public health associations; academic consortia; and nongovernmental organizations.

[7] Centers for Disease Control and Prevention, "Ten Guiding Principles for Data Collection, Storage, Sharing, and Use to Ensure Security and Confidentiality," March 5, 2014, accessed February 3, 2021, https://www.cdc.gov/nchhstp/programintegration/tenguidingprinciples.htm.

[8] Centers for Disease Control and Prevention, "Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing," December 15, 2020, accessed February 3, 2021, https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/guidelines-digital-tools-contact-tracing.pdf.

III. FINDING AND RECOMMENDATIONS

FINDING: CDPH's COVID-19 contact tracing program mitigates data privacy and cybersecurity risks.

In response to the COVID-19 pandemic, the Chicago Department of Public Health (CDPH) developed an electronic case management tool using the Salesforce platform. This tool, called the COVID-19 Assessment and Response Electronic System (CARES), helps 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 their close contacts.

The City of Chicago's Information Security and Technology Policies (ISTP) prescribe the minimum technology security requirements for City departments, and the Information Security Office (ISO) is responsible for reviewing compliance with and enforcement of these standards. The United States Centers for Disease Control and Prevention (CDC) has released multiple guidance documents for public health programs regarding the protection of patients' medical information, particularly contact tracing data collected in response to the COVID-19 pandemic.[9] Referring to ISTP standards and CDC guidance, OIG examined the data privacy and cybersecurity design and practices of CDPH's COVID-19 contact tracing program and the CARES tool.

We found that CDPH's 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.

1. CARES meets the security requirements of the City's Information Security and Technology Policies

The City's ISTP provide departments with standards to mitigate security risks and comply with applicable laws and regulations, such as the Health Information Portability and Accountability Act (HIPAA). City departments must follow these standards and work with the City's ISO to ensure that all technology projects protect the confidentiality, integrity, availability, and accountability of data.

ISO's review of CARES concluded that it met the security requirements of the City's ISTP. OIG spoke with CDPH staff responsible for managing the development of CARES, as well as ISO staff who reviewed the system. We also reviewed documentation of the CARES security features and the process ISO took to conduct its review. The CARES tool includes several features that help mitigate security risks:

[9] Centers for Disease Control and Prevention, "Mission, Role, and Pledge," May 13, 2019, accessed February 26, 2021, https://www.cdc.gov/about/organization/mission.htm.

- A Salesforce platform product that received FedRAMP and HITRUST certification for data protection.
- Active cybersecurity threat monitoring provided by Salesforce.
- Encryption of data in transit and at rest.[10]
- The ability to monitor system usage, and create reports and audit trails.

2. CARES access controls meet the security requirements of the City's Information Security and Technology Policies, but CDPH did not promptly remove access for all terminated users

The ISTP require a department to allow only the minimum access necessary for each information system user. The access controls should reflect the sensitivity and risk of the relevant data. Moreover, the department should have a formal process for granting access to individuals and should document its access decisions.

ISO reviewed CDPH's access controls for CARES and determined they meet the security requirements of the City's ISTP. OIG spoke with CDPH staff and reviewed documentation to understand the access control features of CARES, as well as the policies and procedures implementing those controls. We also spoke with ISO staff and reviewed documentation to understand its access review process. Access control features include,

- multi-factor system access authentication for users through Okta;[11]
- a role-based security matrix that defines system use categories called "personas" and defines each persona's usage permissions and restrictions within CARES;
- a list of CARES users with their persona designation; and
- defined procedures for granting, changing, and terminating access to CARES.

OIG reviewed the authorized users of CARES and determined that, as of January 11, 2021, CDPH assigned all users a persona defined within the role-based security matrix. This means that each user's permissions should provide only the minimum access necessary for their role, meeting the requirements of the ISTP.

Finally, OIG reviewed CDPH's process for and history of terminating accounts to ensure that contact tracers who were terminated or resigned had their access to CARES removed within seven days, in accordance with ISTP timeliness standards. As of February 15, 2021, 50 contact tracers had been terminated or resigned from their position. Of these, only 11, or 22%, had their access to CARES removed by the Department within 7 days. We also found that 13, or 26%, of these individuals still had access to CARES as of March 15, 2021. However, CDPH provided a user

[10] Encryption translates data from readable to non-readable form to prevent unauthorized viewing.
[11] Multi-factor Authentication is an added layer of security used to verify an end user's identity when they sign in to an application. For example, authorized users can register a personal device, such as a cell phone, that will receive an "accept/reject" notification whenever the user attempts to log into a system. This allows the user to verify their identity. Okta, "About Multifactor Authentication," 2021, accessed March 3, 2021, https://help.okta.com/en/prod/Content/Topics/Security/mfa/about-mfa.htm.

activity report demonstrating that none of these individuals logged in to CARES after their employment ended.

CDPH management stated that the delay in user termination is caused by resource constraints and balancing several high-risk priorities. Management said it is important to limit the ability to create or remove system access to a small number of people. In this case, it is limited to one member of senior management who is responsible for overseeing the entire COVID-19 contact tracing program and has responsibilities that often take precedence over terminating access. Moreover, the system administrator position—which could assist with this task—is currently vacant. As CDPH management demonstrated, their ability to monitor users' activity in CARES mitigates some of the risks of delayed access termination.

3. Training for contact tracers aligns with the City's Information Security and Technology Policies, and CDPH maintains a record of all contact tracers' completion of training

The ISTP require departments to train new employees on information security measures. OIG found that CDPH's training for contact tracers met this standard. We spoke with CDPH management who worked with Malcom X College, the University of Illinois at Chicago, Sinai Health, and the Illinois Department of Public Heath to develop and administer training. We also reviewed the training curriculum, which includes several elements to develop understanding of data privacy and information security principles. In particular, the training covers:

- Public health ethics, privacy, confidentiality, and security.
- Relevant federal and state statutes and regulations in the context of the proper collection, transmission, storage, and maintenance of confidential information.
- Proper handling of personal health information (PHI) and personally identifiable information (PII).
- Strategies to create a productive work environment that promote data privacy and cybersecurity.
- Proper use of the CARES system.

CDPH created a library with training and guidance materials within Microsoft Teams that contact tracers use to quickly access materials when needed. OIG also determined that, as of December 16, 2020, CDPH had a record of all contact tracers' completion of training prior to beginning work.

4. CARES prompts contact tracers to inform individuals that all information will be confidential and secure, and requires individuals' consent to be recorded, but does not prompt notification of how long the City will store the information

In its guidance for the implementation of electronic contact tracing tools, CDC advises that public health departments engaged in contact tracing inform persons diagnosed with a disease and

their contacts about what data will be collected, how it will be used, and how long it will be retained. Contact tracers also must receive consent to collect and use personal information.[12]

OIG spoke with a team supervisor to understand how contact tracing staff perform their jobs. We also reviewed the CARES call script and data dictionary to understand what information is provided during a call and which questions are required to be asked. We found that CARES requires staff to obtain consent. The call script also prompts contact tracers to provide a brief overview of COVID-19, and to explain that all information provided will be confidential, stored in a secure location, and will not be shared with individuals not involved in their care. However, the call script does not provide details on how long the City will retain information gathered, which is recommended by the CDC.

5. CDPH has policies to mitigate risks when exchanging confidential information through electronic communications

The ISTP require that City departments develop policies to mitigate risks when exchanging information. Specifically, they state that any information deemed confidential should not be sent via electronic communication unless the message is encrypted, and that employees, contractors, and City partners must be reminded of their responsibility to use City systems appropriately.

CDPH has several procedures to mitigate the risk that confidential information will be exposed through electronic communications. Department management stated that their goal was for the COVID-19 contact tracing program to protect PHI, PII, and other confidential information. CDPH trains contact tracers to never include PHI or PII in electronic communication. If they must refer to a specific case, they are trained to use unique client codes. Day-to-day communications are conducted through group chats in Microsoft Teams, a business communication platform, which encrypts all communications in transit and at rest within Microsoft data servers. These group chat conversations include supervisors, which helps CDPH management ensure that PHI and PII are not transmitted electronically.

6. CDPH has policies that designate persons responsible for reviewing data requests, but does not provide explicit criteria for determining whether to release data

CDC has adopted standards to facilitate data sharing, which state that public health organizations should "limit sharing of confidential or identifiable information to those with a justifiable public health need."[13]

CDPH has policies that designate position titles responsible for reviewing data requests, explain how to share sensitive public health data, and establish procedures for addressing public health ethical concerns, including those related to data sharing. However, the data release policy does not include explicit criteria for Department staff to determine whether to release data. Without

[12] Centers for Disease Control and Prevention, "Guidelines for Digital Tools," 4.
[13] Centers for Disease Control and Prevention, "Standards to Facilitate Data Sharing," Principle 3.

specific guidance, staff may release data inconsistently, or in a manner that conflicts with management's expectations.

RECOMMENDATIONS

1. CDPH should adjust its process for removing access to CARES to ensure it is completed within seven days of a user's termination. The Department might look for opportunities to automate this process.
2. CDPH should update the CARES call script to inform patients and contacts how long the City will retain their data.
3. CDPH should update their data release policy to include explicit criteria for staff to reference when determining whether to grant data requests.

MANAGEMENT RESPONSE

1. *"CDPH currently uses automated reports from the CARES system to help program managers know who has logged in and is active in the system, and in this way, monitors activity for all users. Through this process, CDPH is able to ensure no inactive users, including terminated employees, are actually accessing the system and its records on a regular basis.*

   "To address this recommendation, CDPH and the Chicago Cook Workforce Partnership ("Partnership") will incorporate employment status reviews into its weekly check-ins with the community-based organizations that are in the corps. This will help ensure CDPH is notified when an employee has left the corps and enable the prompt termination of the employee's access to the system.

2. *"CDPH will create a data retention policy for CARES and will update the call script to inform interviewees how long their data will be retained.*

3. *"CDPH will create criteria to guide its privacy officer on release of data in response to data requests."*

IV. OBJECTIVE, SCOPE, AND METHODOLOGY

A. OBJECTIVE

The objective of the audit was to determine if CDPH mitigated privacy and security risks associated with the collection, storage, and transmittal of COVID-19 contact tracing data in accordance with ISTP and CDC guidance.

B. SCOPE

This audit assessed the data privacy and cybersecurity policies and practices of the COVID-19 Community-Based Contact Tracing program and reviewed the CARES electronic case management tool. It did not assess the design or implementation of contact tracing as an activity performed by CDPH or its community partners.

C. METHODOLOGY

To identify criteria for measuring the design and performance of the CDPH's contact tracing program, we reviewed guidance produced by CDC and the City of Chicago's ISTP. We also spoke with the City's chief information security officer.

To assess CDPH's program design for data privacy, we interviewed a contact tracing team supervisor and reviewed the call script used by contract tracers to determine if it provided patients and contacts with information on what data would be collected and how it would be used and stored, and whether it prompted the required request for consent.

To assess CDPH program design for evaluating data requests, we interviewed the Department's HIPAA privacy officer and reviewed data release policy and procedure documents.

To assess the contact tracing program's cybersecurity and access controls, we interviewed CDPH staff responsible for designing CARES, then reviewed documentation of the program's access, data storage and transmission, communication, and process controls. We also spoke with information technology subject matter experts within the City's Department of Assets, Information and Services (AIS) and reviewed their technology assessment of CARES' compliance with the City's ISTP.

To determine if CDPH removed access to CARES within seven days for all contact tracers who were terminated or resigned, we reviewed a report generated by the Chicago Cook Workforce Partnership which listed all such contact tracers and recorded their last day of employment. We compared the dates of last employment to a report from CARES listing active and terminated accounts, which included a timestamp showing when account access was removed for each terminated account.

To assess the Department's program design for protecting confidential information contained in electronic messages, we spoke with CDPH management and contact tracing staff, reviewed Department policies and training regarding protection of confidential information through electronic communication, and spoke with subject matter experts within AIS.

To assess CDPH's program design for training contractors on data privacy and cybersecurity principles, we interviewed a contact tracing supervisor and Department personnel who developed the program. We then reviewed the training curriculum to determine if it aligned with the requirements of the City's ISTP. Finally, we reviewed CDPH documentation to ensure that all contractors received training prior to engaging in contact tracing activities.

OIG considered three components of internal control in our evaluation of the COVID-19 contact tracing program's data privacy and security. Specifically, we examined control environment principles related to the design and implementation of the contact tracing program; control activities principles related to the design, implementation, and operating effectiveness of program policies and training, and information security controls for the Chicago CARES tool; and information and communication principles related to the design of program policies and procedures for data collection and sharing.

D. STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

E. AUTHORITY AND ROLE

The authority to perform this audit is established in the City of Chicago Municipal Code § 2-56-030 which states that OIG has the power and duty to review the programs of City government in order to identify any inefficiencies, waste, and potential for misconduct, and to promote economy, efficiency, effectiveness, and integrity in the administration of City programs and operations.

The role of OIG is to review City operations and make recommendations for improvement.

City management is responsible for establishing and maintaining processes to ensure that City programs operate economically, efficiently, effectively, and with integrity.

The City of Chicago Office of Inspector General (OIG) is an independent, nonpartisan oversight agency whose mission is to promote economy, efficiency, effectiveness, and integrity in the administration of programs and operations of City government. OIG achieves this mission through,

- administrative and criminal investigations by its Investigations Section;
- performance audits of City programs and operations by its Audit and Program Review Section;
- inspections, evaluations and reviews of City police and police accountability programs, operations, and policies by its Public Safety Section; and
- compliance audit and monitoring of City hiring and human resources activities by its Compliance Section.

From these activities, OIG issues reports of findings and disciplinary and other recommendations to assure that City officials, employees, and vendors are held accountable for violations of laws and policies; to improve the efficiency, cost-effectiveness government operations and further to prevent, detect, identify, expose and eliminate waste, inefficiency, misconduct, fraud, corruption, and abuse of public authority and resources.

OIG's authority to produce reports of its findings and recommendations is established in the City of Chicago Municipal Code §§ 2-56-030(d), -035(c), -110, -230, and 240.

PROJECT TEAM

Kevin Smith, Senior Performance Analyst
Samuel Díaz, Performance Analyst
Cameron Lagrone, Chief Performance Analyst

PUBLIC INQUIRIES

Communications: (773) 478-8417 | communications@igchicago.org

TO SUGGEST WAYS TO IMPROVE CITY GOVERNMENT

Visit: igchicago.org/contact-us/help-improve-city-government

TO REPORT FRAUD, WASTE, AND ABUSE IN CITY PROGRAMS

Call OIG's toll-free hotline: (866) 448-4754 / TTY: (773) 478-2066
Or visit: igchicago.org/contact-us/report-fraud-waste-abuse/

Cover image courtesy of iStock.
Alternate formats available upon request.