REPORT OF EXAMINATION | 2022M-146

Cayuga County

Security of Electronic Public Health Department Personal, Private and Sensitive Information

DECEMBER 2022

OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

Report Highlights

Cayuga County

Audit Objective

Determine whether Cayuga County (County) officials ensured electronic data containing personal, private, and sensitive information (PPSI) on County-owned Public Health Department (Department) devices was adequately protected from unauthorized access and use.

Key Findings

County officials did not adequately protect the Department's electronic data containing PPSI. In addition to sensitive information technology (IT) control weaknesses communicated confidentially to officials, we found:

- Electronic data containing PPSI on 32 of the 61 County-owned Department IT devices we examined, in violation of County policies.
- County officials have not established a County-wide data classification schematic and have not inventoried PPSI in their possession.
- County officials and IT staff did not establish formal written procedures to help adequately secure PPSI.

Key Recommendations

- Ensure IT policies and procedures are consistently and appropriately followed.
- Establish a data classification inventory that assigns the appropriate security level to each type of data.
- Develop formal written procedures to help ensure PPSI is adequately secured.

County officials agreed with our recommendations and indicated they planned to initiate corrective action.

Background

The County is located in the central part of New York State. The County encompasses 23 towns, nine villages and one city. The County is governed by the County Legislature (Legislature), which is composed of 15 elected members, one of whom serves as the Chair. The Legislature is responsible for the general oversight of financial affairs and safeguarding resources.

The Chief Information Officer (CIO) oversees the County's IT environment, including controls over electronic data containing PPSI. The current CIO was appointed in July 2021. The Department is overseen by the Director of Public Health (Director) who is responsible for ensuring that PPSI used, transmitted, accessed and shared by the Department is protected.

Quick Facts	
2021-22 IT Budget	$2.5 million
Department Staff	107
Department IT Devices	137

Audit Period

January 1, 2021 – June 22, 2022

Security of Electronic Public Health Department Personal, Private and Sensitive Information

County officials and staff rely on the County's IT assets for maintaining confidential and sensitive financial, personnel and health records, email and Internet access. In addition, county health departments typically possess PPSI such as personally identifiable information, health and medical records, early intervention student information and payroll information. PPSI is information in which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have or cause a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

How Should County Officials Secure Electronic Department Data To Help Prevent Unauthorized Access to PPSI?

County officials are responsible for ensuring that PPSI is properly safeguarded and is used only for business purposes. To help officials fulfill this responsibility, it is essential for the legislative body to adopt comprehensive written IT security policies to help protect PPSI that is accessed and stored on IT devices, such as desktops, laptops, tablets and smartphones. Furthermore, it is the responsibility of county officials and IT staff to ensure the legislature's policy directives are met by establishing procedures and communicating these to staff members who use IT devices to access or store PPSI. It is also important that county officials know about all the types of data they possess, access and maintain on IT devices so they can make informed decisions about setting appropriate security levels. To do this, county officials should maintain an inventory of data stored on their IT devices to help account for the PPSI they maintain.

Effective policies and procedures should be developed and implemented for protecting PPSI to address various aspects of securing confidential data and limiting access to it. Data should be inventoried and classified according to its sensitivity. Because different kinds of information require different levels of protection, the nature of the data has to be evaluated so that appropriate internal controls can be established and monitored. The data classification process assigns data to a category that will help determine the level of internal controls over that data. In some instances, laws, regulations or an organization's policies predefine the classification of each data type. County officials should update the classification and inventory list routinely to reflect any changes. In the event of a data breach, the proper classification and inventorying of PPSI helps allow officials to determine the extent of unauthorized access and take appropriate action.

Effective policies and procedures should be developed and implemented for protecting PPSI to address various aspects of securing confidential data and limiting access to it.

County Officials Did Not Adequately Secure Electronic Department Data

Officials developed and the Legislature adopted written policies to help protect the County's PPSI, specifically related to email, storage and disposal. The County's policies also state that, prior to disposing of devices, staff should ensure all PPSI

is destroyed or removed. In addition, no employee shall access or store County data of any kind using an unauthorized IT device, and all County-related data is to be stored on the County's shared network drives and not on a device's local hard drive. However, while the County's IT Department had some informal procedures in place, County officials and IT staff had not developed formal specific written procedures, in accordance with the Legislature's directive, to help ensure PPSI was consistently protected from exposure and unauthorized access.

As a result of the County's lack of formal and consistent IT procedures, and the unique nature and volume of PPSI that the Department accesses and uses, we examined County-owned IT devices assigned to Department staff for the presence of PPSI and whether County officials had adequately secured this data. We examined 61 devices and found that 32 (52 percent) contained at least one form of PPSI, with some IT devices having multiple forms of PPSI, stored on local hard drives. We determined that while the information stored on these devices was business related, it was in violation of the County's policies to be stored on the devices' local hard drives. We did find that IT staff had implemented certain controls to help safeguard PPSI on Department IT devices which helped to restrict access to authorized users, such as requiring passwords on all devices and restricting administrative rights. Due to employees' lack of awareness of the policy requirements, the CIO and Director indicated that training would be provided to staff to ensure the storage of data is in accordance with County policies.

We determined that while the information stored on these devices was business related, it was in violation of the County's policies to be stored on the devices' local hard drives.

Additionally, County officials have not established a County-wide data classification schematic and have not inventoried the PPSI in their possession. As a result, County officials do not know to what extent PPSI resides on County devices.

Written procedures with clear instructions for staff to follow help ensure that privileged information is not acquired by a person without valid authorization. When officials do not develop and implement comprehensive written procedures for these key areas, communicate them to applicable staff and continually monitor and update them as necessary, the risk that unauthorized users could access and misuse confidential data, such as PPSI in health and medical records, early intervention student records, or payroll information, without detection is significantly increased.

Furthermore, without classifying data, and setting appropriate security levels for PPSI, there is an increased risk that PPSI could be inadvertently exposed to unauthorized users. Additionally, the lack of information about the types and extent of data the County maintains can hamper efforts to properly notify affected parties in the event of a data breach.

What Do We Recommend?

The CIO and IT staff should:

1. Develop formal written procedures to help ensure PPSI is adequately secured, which outline proper access, transmission, storage and usage of PPSI.

2. Establish a data classification schematic for the types of information the County maintains and assign an appropriate security level to each type of data; then conduct an inventory of PPSI stored to account for the confidential data maintained and ensure this inventory list is updated on an ongoing basis.

The CIO, IT staff and Director should:

3. Ensure IT policies and procedures are consistently and appropriately followed to help facilitate the protection of PPSI.

4. Ensure that training is provided to employees to help ensure they understand and follow policy requirements.

Appendix A: Response From County Officials

County of Cayuga

David S. Gould
Chair Cayuga County Legislature
160 Genesee St.
Auburn, NY 13021

November 18, 2022

Dear Mr. Grant:

This letter is in response to the Draft Report of Examination: Security of Electronic Public Health Department Personal, Private and Sensitive Information (PPSI), which was reviewed and discussed with me, the Chief Information Officer (CIO), and the Director of Public Health at the exit conference held on November 9, 2022. We valued the opportunity to discuss the outcomes of your examination and to learn more about best practices that could be implemented to further ensure data privacy on County-owned devices.

The period covered by this examination is January 1, 2021 – June 22, 2022, which was a challenging time within the County Information Technology (IT) Department as we worked to transition away from a managed IT service provider in favor of all County hired staff, starting with the CIO who was hired in July of 2021. The primary function of the CIO was to completely overhaul the department as well as the County IT infrastructure, while also keeping IT data security at the forefront.

We appreciate the recommendation that all IT policies and procedures are consistently and appropriately followed, and that the County continue to develop formal written procedures to help ensure PPSI is adequately secured. When the CIO took the role in July of 2021, all IT policies and procedures were carefully reviewed. These documents will be continued to be reviewed and updated over the course of next several months to ensure they are as current and relevant as possible.

Additionally, the recommendation to establish a data classification inventory is something that will be extremely helpful to inform our risk management process, prioritize security measures, reduce data maintenance and storage costs, improve overall IT security.

We are actively working on developing our corrective action plan which will include the full plan and process to implement your suggestions. Our goal is to provide this back to you immediately following Legislative approval.

Thank you for your field staff's assistance and thoughtful feedback concerning data and security on County-owned devices. Your team's willingness to engage with us to help improve our practices is very much appreciated.

Respectfully,

[redacted]

David Gould
Cayuga County Legislature Chair
District 5 Representative

160 Genesee Street, Auburn, New York 13021- Office (315) 253-1273 Cell (315) 246-3042 - E-mail: dgould@cayugacounty.us

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We interviewed County officials and staff and reviewed relevant IT policies and procedures, as well as security controls in place to gain an understanding of the County's IT environment and the IT environment within the Department.
- On May 10, 2022, May 12, 2022 and May 16, 2022, we reviewed a sample of 61 County-owned IT devices assigned to Department staff to determine whether PPSI was present on the local hard drive, and whether controls were in place to help secure PPSI stored locally. We selected our sample by obtaining a list of County staff and determining which staff were full- or part-time within the Department. We selected 100 percent of the full-time staff (34 total) and randomly selected using a random number generator an additional six part-time staff of those who were assigned devices for a total of 40 Department employees selected. We then reviewed all IT devices assigned to the selected staff members.
- We ran computerized audit scripts on May 3, 2022 on servers and domain controllers pertinent to the Department to determine information pertaining to access rights and controls.

Our audit also examined the adequacy of certain IT controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to County officials.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or size of the relevant population and the sample selected for examination.

The Legislature has the responsibility to initiate corrective action. A written corrective action plan (CAP) that addresses the findings and recommendations in this report should be prepared and provided to our office within 90 days, pursuant to Section 35 of General Municipal Law. For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Legislature to make the CAP available for public review in the Clerk of the Legislature's office.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/files/local-government/pdf/regional-directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/files/local-government/publications/pdf/cyber-security-guide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller
www.osc.state.ny.us/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.ny.gov

www.osc.state.ny.us/local-government

Local Government and School Accountability Help Line: (866) 321-8503

ROCHESTER REGIONAL OFFICE – Edward V. Grant Jr., Chief of Municipal Audits

The Powers Building • 16 West Main Street – Suite 522 • Rochester, New York 14614-1608

Tel (585) 454-2460 • Fax (585) 454-3545 • Email: Muni-Rochester@osc.ny.gov

Serving: Cayuga, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates counties

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller