

**Quarterly Report of the Chief Privacy Officer  
on Agency Disclosures  
Made Under Exigent Circumstances or  
in Violation of the Identifying Information Law\***

**Reporting Period: September 16, 2020 through December 15, 2020**

\*This report is compiled in accordance with the requirements of Section 23-1202 of the New York City Administrative Code, which requires the Chief Privacy Officer to submit a quarterly report containing an anonymized compilation or summary of such disclosures to the Speaker of the City Council.

Description	Total
<b>Total number disclosure(s) reported by agencies as made under exigent circumstance(s):</b> (N.Y.C. Admin. Code § 23-1202(d)(2))	1
<b>Total number of disclosure(s) reported by agencies as made in violation of the Identifying Information Law:</b> (N.Y.C. Admin. Code § 23-1202(c)(4))	20

For the reporting period September 16, 2020 through December 15, 2020, City agencies and offices have reported any collections and disclosures made under exigent circumstances, and disclosures made in violation of the Identifying Information Law, as summarized below.

Type of disclosure reported	Summary description
Disclosure in Violation of the Identifying Information Law	Agency learned about a technical error in its online database service that allowed clients to improperly access to certain information about other clients. Agency reported immediate investigation by its information technology department and resolution the same day by turning off and promptly repairing the impaired technical component. The agency is working with their legal department to determine the data elements that were improperly accessed due to the technical issue, to determine any client notifications to be made.
Disclosure in Violation of the Identifying Information Law	Agency reported a ransomware attack on one of their contracted service providers. The provider hired a third-party investigator, which secured the files and rebuilt the network. The agency reported the matter to relevant local and federal authorities. The agency also engaged in a further investigation and risk assessment in collaboration with the CPO, Cyber Command, other City officials, and the provider to determine any necessary notifications and offers of credit monitoring.
Disclosure in Violation of the Identifying Information Law	Agency employee reported that their personal desktop computer (utilizing remote access from their agency-issued laptop) had been compromised by an unknown bad actor. The employee immediately notified their supervisor who subsequently reported the matter to the agency's data security team and NYS Cyber Command Center. The agency reported remedial measures to enhance security and continues to investigate the incident to determine scope of any confidential information accessed and any notification requirements.
Disclosures in Violation of the Identifying Information Law (8)	In eight instances, agency mailed documents to one client that were intended for another client. The agency is notifying the individuals whose identifying information was disclosed. Agency reported remedial measures to enhance internal security protocols and quality assurance review.

Disclosure in Violation of the Identifying Information Law	Agency reported that information of clients and one of the minor children of a client was improperly disclosed to another recipient. Agency reported an ongoing investigation to understand the mechanism of disclosure.
Disclosure in Violation of the Identifying Information Law	Agency employee inadvertently emailed client information to an improper recipient. Agency reported working with the Chief Privacy Officer to draft a notification letter to the affected clients.
Disclosure in Violation of the Identifying Information Law	Agency employee inadvertently emailed client information to another agency instead of the intended recipient. The sending agency immediately notified the improper recipients of the error and requested that the email containing client information be deleted immediately. The improper recipients all confirmed that the email had been deleted. The sending agency reported enhanced internal security protocols and quality assurance review.
Disclosure in Violation of the Identifying Information Law	Agency contractor reported a security incident at one of their offices, also reported to police, where one or more individuals broke into the facility and stole multiple items including a USB drive containing client information. Agency and the provider collaborated with the CPO and other City officials to determine scope of disclosure, remedial actions, and notification letter to affected clients.
Disclosures in Violation of the Identifying Information Law (4)	In four instances, agency mailed documents to one client that were intended for another client. In one additional instance, the agency reported that an employee handed documents containing client information to an improper recipient. The agency notified the individuals whose identifying information was disclosed.
Disclosure in Violation of the Identifying Information Law	Agency conducted an online survey where clients could ask questions or provide input. The online survey was circulated with a setting that allowed those who submitted the form to see the other submissions. Agency reported turning off that setting as soon as they discovered the issue.
Disclosure Made Under Exigent Circumstances	Agency shared urgent health related identifying information of an employee with another agency prior to having such disclosure first approved by the agency privacy officer. The agency privacy officer has since developed an approved protocol for this type of disclosure prospectively.

**Submitted by:** \_\_\_\_\_  
 Laura Negrón  
 Chief Privacy Officer, City of New York

**Date:** December 29, 2020