

# INCIDENT REPORTING AND NOTIFICATION

Educational agencies shall report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer and notify impacted stakeholders. To learn more about this requirement, agencies can review Part 121.10 of the Regulations.

## REQUIREMENTS FOR NYS EDUCATIONAL AGENCIES



### COMPLIANCE CHECKS

**Incident Response Procedures:**

- ✓ Outlines All Required Actions

**Contracts:**

- ✓ Outline All Third-Party Contractor Requirements



### REPORTING REQUIREMENTS



#### 10 DAYS TO REPORT TO NYSED

The agency must report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer no more than 10 calendar days after such discovery.

### NOTIFICATION REQUIREMENTS



#### 60 DAYS TO NOTIFY AFFECTED INDIVIDUALS

The agency must notify affected parents, eligible students, teachers and/or principals no more than 60 calendar days after the discovery of a breach or unauthorized release.



#### LAW ENFORCEMENT OR VULNERABILITY DELAY

Where notification is delayed, the agency must notify affected individuals within 7 calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.



#### THIRD-PARTY REIMBURSEMENT REQUIREMENT

Where a breach or unauthorized release is attributed to a third-party contractor, the contractor must pay for or reimburse the agency for the full cost of notification.



#### METHOD OF NOTIFICATION

Notification must be directly provided to the affected individuals by first-class mail to their last known address; by email; or by telephone.



#### CONTENTS OF NOTIFICATION

Notifications must be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

- a brief description of the unauthorized release
- the dates of the incident and date of discovery
- a description of the types of PII affected
- the number of records affected
- a brief description of the agency's investigation
- contact information for representatives who can assist parents



## **MODEL IMPROPER DISCLOSURE NOTIFICATION**

This letter is to inform you of an incident that occurred within the [insert system]. This incident resulted in student/staff/etc data being accessed without authorization by an outside entity. Our Incident Response Team acted quickly to assess and mitigate the situation.

[insert required elements:

- a brief description of the breach or unauthorized release
- the dates of the incident and the date of discovery
- a description of the types of personally identifiable information affected
- an estimate of the number of records affected
- a brief description of the educational agency’s investigation or plan to investigate]

Please know that our district is committed to protecting and securing educational data. Our team has extensive training in data security and privacy, and our systems have many controls in place to protect your child’s educational records. Our team is working with a group of experts to review the incident and implement appropriate measures to protect against this type of incident occurring in the future. Please contact [insert name] with any questions you may have regarding this incident and our response [Note: The regulations require agencies to include contact information for representatives who can assist parents].

## **MODEL UNAUTHORIZED RELEASE COMPLAINTS RECORD**

The agency must maintain a record of all complaints and their disposition in accordance with applicable data retention policies, including ED-1. Insert information about complaints into the log.

<b>COMPLAINANT NAME</b>	<b>DATE COMPLAINT SUBMITTED</b>
<b>DESCRIPTION OF THE COMPLAINT</b>	
<b>FINDINGS</b>	
<b>DATE THE FINDING REPORT WAS SHARED WITH COMPLAINANT</b>	