Controlled Reports and PII

Last Modified on 10/22/2022 10:13 am CDT

Understanding PII

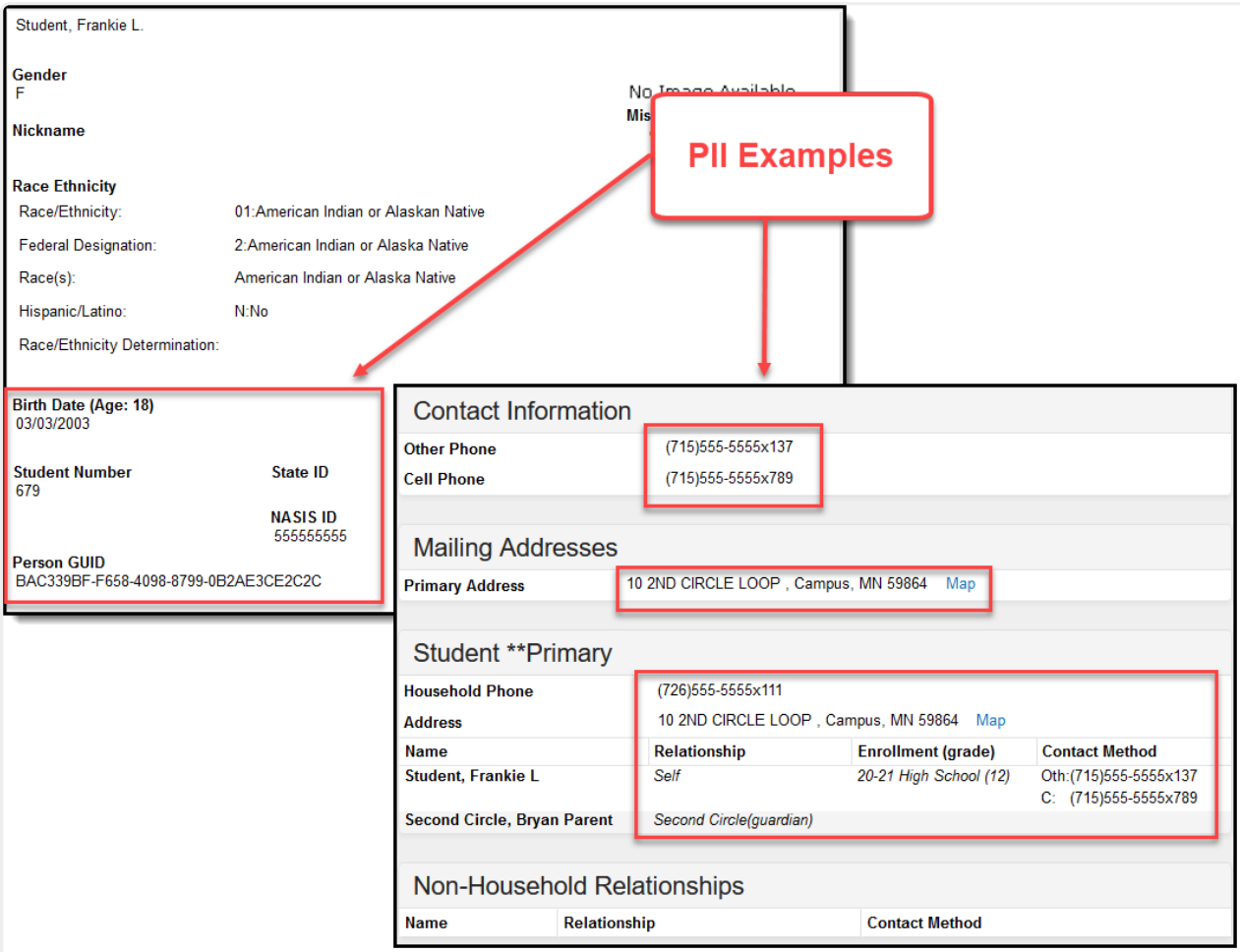
PII (Personally Identifying Information) is any private or sensitive information that can be used to personally identify an individual. As a Student Information System, Campus has many locations where PII data exists. To protect this information, every tool and report in Campus is guarded by set of tool and calendar rights to prevent unauthorized access. However, even with strong safety measures in place, PII can still be compromised if a user doesn't do their part in keeping sensitive data secure. It is critical that every Campus user understand the role they play in protecting PII.

Personal Impacts when PII is compromised

Fraudulent activity such as identity theft can cause substantial damages to a person if their PII is compromised. PII is considered to be compromised when a person has gained access to information they are not authorized to have access to. Once compromised, PII can be used for:

- Opening a new credit card or loan
- Opening a bank account
- Other fraudulent activities

Examples of PII include: Social Security Numbers, birth dates, physical addresses, and other forms of ID a person may use. In Campus, PII is viewable in areas such as Demographics and Census. Data in these locations may be used in state reports and is available for extract in Ad hoc Reporting.



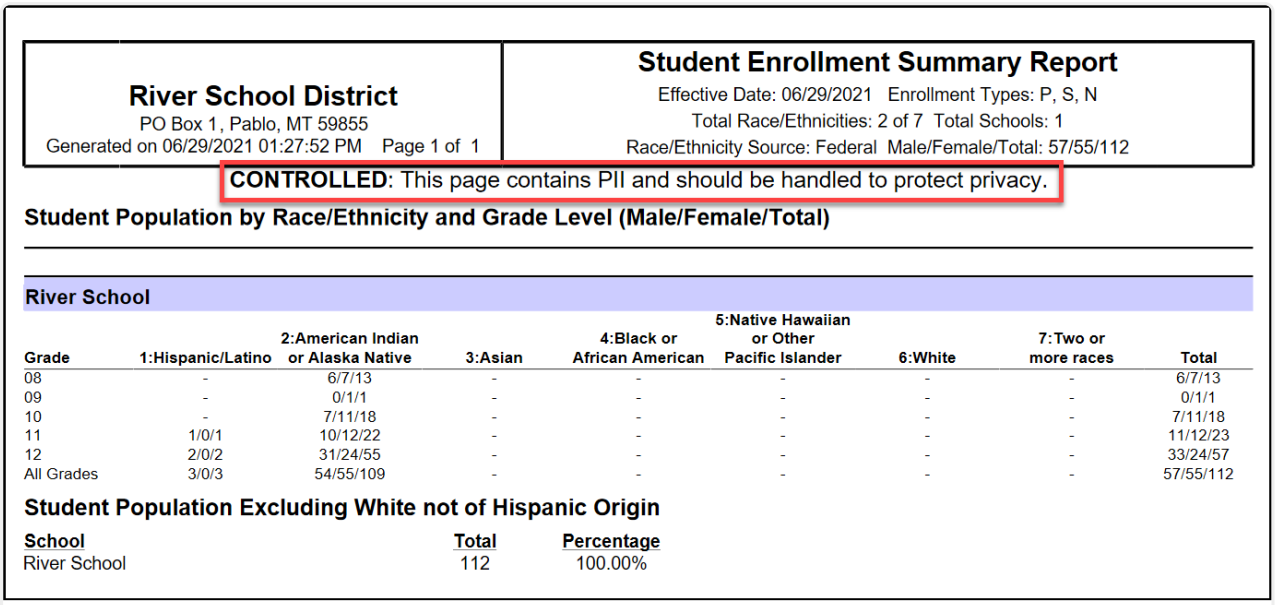
Examples of PII

Identifying Reports Containing PII

For the purposes of accurate reporting and identification, many reports available in Campus include PII. As a precautionary measure, reports containing PII display a **CONTROLLED** security statement in the report header for PDF and DOCX formats. For CSV and TXT formats, a file name indicating Controlled Unclassified Information (CUI) is included in the report. A report in CSV format with PII has a file name of SampleReport_CUI.csv; a report in TXT format that includes PII has a file name of SampleReport_CUI.txt.

Users should follow their school district's policy when viewing reports where CONTROLLED displays and where the file name indicates PII exists.

The CONTROLLED statement only displays in reports containing PII for BIE schools and NASIS.



River School District
PO Box 1, Pablo, MT 59855
Generated on 06/29/2021 01:27:52 PM Page 1 of 1

Student Enrollment Summary Report
Effective Date: 06/29/2021 Enrollment Types: P, S, N
Total Race/Ethnicities: 2 of 7 Total Schools: 1
Race/Ethnicity Source: Federal Male/Female/Total: 57/55/112

CONTROLLED: This page contains PII and should be handled to protect privacy.

Student Population by Race/Ethnicity and Grade Level (Male/Female/Total)

River School

Grade	1:Hispanic/Latino	2:American Indian or Alaska Native	3:Asian	4:Black or African American	5:Native Hawaiian or Other Pacific Islander	6:White	7:Two or more races	Total
08	-	6/7/13	-	-	-	-	-	6/7/13
09	-	0/1/1	-	-	-	-	-	0/1/1
10	-	7/11/18	-	-	-	-	-	7/11/18
11	1/0/1	10/12/22	-	-	-	-	-	11/12/23
12	2/0/2	31/24/55	-	-	-	-	-	33/24/57
All Grades	3/0/3	54/55/109	-	-	-	-	-	57/55/112

Student Population Excluding White not of Hispanic Origin

School	Total	Percentage
River School	112	100.00%

Example of "Controlled" in a Report Header

Who Can See PII

Authorized Users

In Campus, anyone who has been assigned tool rights to view student data or generate reports may be eligible to see the PII of students, staff, and others (parents, guardians, emergency contacts, etc.). It is important to review and follow the policies enforced by your school district when viewing PII.

Unauthorized Users

Unauthorized users are individuals who do not have permission to access the information to which they have gained access. Unauthorized users may gain access when PII handling negligence occurs by an authorized user. Examples of PII negligence include: not locking your workstation before leaving it unattended, lending out your username and password, printing a **Controlled** report and leaving it in an area where unauthorized users may see it, and not properly disposing of documents containing PII.

Additional Precautions to Protect PII

It is important to always follow the policies enforced by your school district when viewing or working with PII. Here are a few examples of ways you can help to reduce the risk of compromising PII:

All Users:

- Never leave your workstation unattended when PII is displayed or can be easily accessed.

Consider locking your computer even when trips away from it are brief.
- Never leave a printed report that contains PII in a location where it can be stolen, including sitting on a communal printer.
- Never provide your password to another user who may have restricted or less tool rights than you.
- Never save a downloaded report containing PII on a shared server where others may be able to see it.

Administrative Users:

- Review and assign only the tool rights a user needs to perform the tasks of their job.
- Restrict who is authorized to be given the Student Information System Administrative role.
- Disable user accounts for employees who have left.
- Review tool rights for employees who are changing roles in the school/district.