Trump Announcement on Public Benefits Does Not Change Legal Protections for K–12 Students

Last updated: August 25, 2025

When students enroll in school and in school-related services, they shouldn't have to worry about whether their private information will be used against them. Protecting students' private information keeps students safe and helps prevent their data from being misused. Schools should be guardians of sensitive student data. However, recent interpretive notices from the U.S. Departments of Education and Health and Human Services regarding immigrants' potential eligibility for certain federally funded programs has caused confusion and concern.

What is happening?

Per the interpretive notices, agencies that administer certain federal public benefit programs may be required to verify benefit recipients' eligibility based on their immigration status. The newly restricted federal programs that may interface with K–12 schools include the following:

Department of Education Programs

- Career and Technical Education (CTE) programs
- Adult Education and Family Literacy Act (AEFLA) of the Workforce Innovation and Opportunity Act (WIOA)

Department of Health and Human Services Programs

- Community Mental Health Services Block Grant
- Community Services Block Grant (CSBG)
- Head Start
- Health Center Program
- Mental Health and Substance Use Disorder Treatment, Prevention, and Recovery Support Services Programs administered by the Substance Abuse and Mental Health Services Administration
- Substance Use Prevention, Treatment, and Recovery Services Block Grant

While the Department of Education's interpretive notice recognizes the legal protections afforded to undocumented children in K–12 schools under Plyler v. Doe (1982), the administration argues that those protections do not extend to adult education, and therefore, restricting access to those programs does not infringe on Plyler's guarantee of access to a "basic public education." The Department of Health and Human Services notice argues that the Head Start program is "similar to a welfare benefit" and should be restricted for that reason.

Litigation challenging these notices, as well as a Department of Justice determination, is ongoing. Thus, implementation is currently paused in twenty states and the District of Columbia.

For more, see this blog from the National Immigration Law Center.

What could this mean?

To "verify eligibility" for these programs, practitioners could be required to collect information from program beneficiaries. That information might include proof of citizenship or immigration status. However, both notices recognize that under the law, **nonprofit organizations are not required to determine or verify a person's immigration status.**

These notices leave many questions unanswered, including which services are exempt from restriction, how verification might occur if required, and which person's status would be relevant. The notices signal that further guidance may be forthcoming. Providers should not attempt to deny services prematurely, based on assumptions on how they may be implemented.

Why would restricting access to programs be bad for students?

On average, there is at least one cybersecurity incident affecting K–12 schools in the United States per school day. By collecting, storing, and retaining sensitive data such as proof of citizenship or immigration status on all students, schools dramatically increase the likelihood of a data breach of this very sensitive information for all students. According to a study by the U.S. Government Accountability Office, data breaches in K–12 schools contained personally identifiable information, such as Social Security numbers, putting students and families at risk of financial harm.

Collecting and storing unnecessary information about students may also create barriers to education and other critical services. Many U.S. citizens may lack access to documents establishing their status and thus their eligibility; furthermore, retaining immigration status data puts students at risk of surveillance or profiling, which could limit their access. Students and families of all statuses will be concerned about how their sensitive information will be used or protected.

Moreover, policies that discourage student enrollment potentially violate federal law.

What can school districts and service providers do about it?

- ✓ **Do not collect immigration status or citizenship data** from K–12 students.
- ✓ Stay tuned for further guidance, litigation developments, and other changes. Do not deny services prematurely.
- ✓ Depending on what happens, explore other options for structuring programs, segregating funding, and/or securing alternative sources of funding.
- ✓ Develop strong security measures to protect all data and incorporate a plan to safely delete sensitive information when it is no longer needed.
- ✓ Elevate these privacy concerns to program providers, district leaders, and lawmakers.
- ✓ Continue to monitor updated guidance as this rule is implemented in your programs.
- ✓ Consult legal counsel with specific questions or concerns about compliance.
- ✓ Join the National Newcomer Network for more information and resources.

THIS ADVISORY IS NOT LEGAL ADVICE. A SCHOOL, DISTRICT, OR SERVICE PROVIDER SHOULD CONSULT WITH LEGAL COUNSEL ABOUT SPECIFIC CONCERNS.