NATIONAL LEAGUE of CITIES | INSTITUTE FOR YOUTH, EDUCATION & FAMILIES

BUILDING MANAGEMENT INFORMATION SYSTEMS TO COORDINATE CITYWIDE AFTERSCHOOL PROGRAMS

A TOOLKIT FOR CITIES

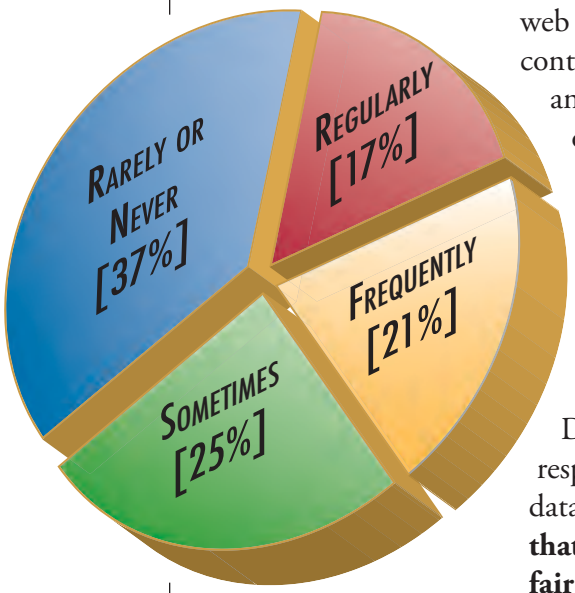
SECTION 3:
DATA STEWARDSHIP: HOW TO PROTECT AND SHARE INFORMATION

Afterschool management information systems process and store a tremendous amount of information on youth participants. Among the crucial responsibilities of an MI administrator is to assure students, parents, and each of the project partners that he or she is a responsible steward of this sensitive information. In practice, this means providing guarantees that the data in the system are "fit for purpose" and that every reasonable precaution has been taken to prevent their misuse.

The specific permissions and prohibitions governing the collection and use of data by an MI system are defined by an overlapping web of federal and state laws, the most prominent of which in the context of afterschool programs is the Family Educational Rights and Privacy Act (FERPA).[1] Untangling the specific application of these laws is not always straightforward.[2]

However, city leaders undertaking this effort should be encouraged by the success of their peers: 67 percent of the cities surveyed by NLC in 2011 have established a framework for sharing information among youth service organizations and schools. Local officials may also be encouraged by the recent FERPA rules issued by the U.S. Department of Education (described on page 45), which responded to some of the most common objections to expanding data sharing relationships with local education agencies. **Cities that can demonstrate a commitment to the principles of fair information practices, that are familiar with how these practices have been embedded in federal law, and that are committed to building trust with school and other information partners can expect to be successful in negotiating access to the data necessary to support their work.**

Chart 5. Information sharing between city coordinating entities and schools



Among the cities surveyed by NLC in 2011, two-thirds of city coordinating entities share information with public schools.

[1] Depending on the type of youth information being shared and how it would be used, other federal laws such as the Health Insurance Portability and Accountability Act (HIPAA) may apply. For a much more detailed description of the interaction of state and federal privacy laws, see the review by Professor John Petrila referenced on page 48 and available through the Intelligence for Social Policy website at www.ispc.upenn.edu.

[2] Though the legal framework for information privacy is complex and changing, it is grounded in a set of international principles that have remained fairly consistent for 40 years and which provide the foundation of privacy law in the United States. These principles are included in Appendix A.

PRIVACY

The Family Educational Rights and Privacy Act (FERPA), section 444 of the federal General Education Provisions Act (GEPA), governs the confidentiality and permitted uses of educational records. In the absence of a more restrictive state statute, this law's provisions determine whether and with whom schools can share student information. FERPA applies to any recipient of funds from the U.S. Department of Education, including local and state education agencies but generally excluding private and parochial schools.

Afterschool providers, city coordinating entities, and third-party program evaluators all fall outside of the list of organizations generally permitted access to student records by FERPA.[3] At least three strategies are available to cities seeking to work within or around this prohibition, however, depending on how the partners intend to use student information:

1. partnering with schools to conduct afterschool evaluations;
2. negotiating designation as an "agent" of the schools to access student information; and
3. requesting prior written permission from each student's parent or guardian to share academic information with providers.

The first two strategies – school-based evaluation and designation as a FERPA-defined "agent" of the schools – are most useful for evaluating programs and overall youth outcomes. These strategies may, for example, allow for a comparison of youth participating in afterschool programs to the general student population and cohorts of non-participating youth.

On the other hand, if the afterschool partnership would like to allow providers access to individual student data for purposes of case management on a day-to-day basis, prior written consent from each student's parent or guardian is required. These three strategies are not mutually exclusive, and each is described in more detail below.

1. Have Schools Analyze Student Data (School-Based Evaluation)

Schools may share information on youth outcomes if it is reported in such a way that no individual student's performance can be determined (see page 48 for a list of information that can be shared). This stipulation permits schools to share data on the performance of their students by cohort, including by school, class, demographic characteristic, or – if they so choose – by participation in afterschool programming. Several citywide afterschool systems, including those in Grand Rapids, Mich., and Nashville, Tenn., are either funding or considering whether to fund a research position within the public schools to serve as a liaison to citywide afterschool partners and conduct this kind of analysis "from inside the FERPA firewall." While this strategy can be very effective, it may not be feasible in cases where afterschool program participants attend multiple school districts or where those school districts are themselves resource-constrained.

[3] Individuals and organizations permitted by default to access student records include students, parents, school officials with a legitimate educational interest, schools to which a student is transferring, parties such as banks connected to student financial aid, accrediting organizations, and state and local authorities pursuant to state law or as related to a health emergency or judicial order.

2. Designate a City Coordinating Entity as an Agent of the Schools (Access to Student Records Without Consent)

Federal regulations (CFR Title 34 § 99.31) define the conditions under which schools may release student records without the prior consent of parents or students, including for purposes of "audit, evaluation, or enforcement or compliance activity" related to education programs, including afterschool programs with an educational focus (see page 48). To quality for this exemption from FERPA, the recipient must qualify as an "authorized representative" of the schools, enter into a written agreement that governs the protection and use of the student data, and identify the local, state or federal law that calls for the audit, evaluation, or compliance activity.[4]

Authorized representatives can include independent consultants, university centers, or city coordinating entities, provided they have executed a written agreement with the agency that addresses the elements described below. **Until recently, FERPA was interpreted as requiring the education agency to have "direct control" over those it authorized to have access to individual student information, and this interpretation limited researchers to being employees or contractors working onsite. A December 2011 rule issued by the U.S. Department of Education eliminated this requirement.**

The written agreement between the schools and their representatives must include, at a minimum:

- Clear designation of the individual or entity being authorized;
- A catalog of specific personally identifiable information (PII) to be disclosed;
- Identification of the purpose for the which the FERPA exemption is being claimed and a description of the activities in sufficient detail to confirm that it is legitimate and could not be accomplished without the disclosure of PII;
- A description of the purpose, scope, and duration of the study;
- The terms under which PII will eventually be returned to the agency or destroyed by the representative, including a timeframe according to which this will be accomplished; and
- Policies and procedures to ensure that PII is not intentionally or accidentally redisclosed or used for any purpose not explicitly permitted in this written agreement.

3. Obtain Permission from Parents (Prior Written Consent)

To inform day-to-day decision making and to share academic information with afterschool providers about individual students, most citywide afterschool systems ask parents and guardians to provide written consent for schools to share information with afterschool

[4] Under this exception, FERPA does not forbid the sharing of student information without consent, but the local or state education agency will have to determine whether it has reason to undertake one of those activities.

providers. Cities generally renew this consent annually, though there are no general prohibitions against requesting consent to share information for two or more years.

Parents' permission can be collected by providers during enrollment or by schools during student registration, and most MI systems will provide a "flag" for each individual student that indicates whether or not this permission has been granted. The consent form provided to parents and guardians should include a list of the specific PII that may be disclosed, should state the purpose of the disclosure, and should clearly identify the organizations (or class of organization) to whom the disclosure may be made.

NEW FERPA RULEMAKING

In December 2011, the U.S. Department of Education amended the regulations governing the implementation of FERPA, primarily to reduce perceived barriers to the appropriate sharing of information for educational purposes. Two changes are of significant interest to afterschool providers:

1. The term "Education Program" is now explicitly defined to include most afterschool programs. This change removes the possible objection that afterschool programs would not qualify for an Evaluation Exemption (using strategy #2 on page 46).

The fine print: Education Programs are defined as any programs that are principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, regardless of whether the program is administered by an educational authority. The rulemaking explicitly includes educational programs conducted by correctional and juvenile justice facilitates, dropout prevention and recovery programs, afterschool programs dedicated to enhancing academic achievement, and high school equivalency programs, "regardless of where or by whom they are administered." However, the rulemaking excludes programs that are principally engaged in recreation and entertainment (so-called "gym and swim").[5]

2. Authorized Representatives no longer need to be under the "direct control" (and supervision) of the schools.

The fine print: Authorized Representatives are defined generally as any entities or individuals designated by a state or local educational authority or an agency headed by an official listed in CFR Title 34 § 99.31(a)(3) – the Secretary of Education, the Comptroller General of the United States, or the Attorney General of the United States – to conduct, with respect to federal or state-supported education programs, any audit, evaluation, or compliance or enforcement activity in connection with federal legal requirements related to those programs. The incorrect interpretation by many education agency legal counsels that this representative must be under the "direct control" of the authorizing agency and therefore limited to agency staff and direct contractors has been clarified by the recent FERPA rulemaking; there is no such requirement.

[5] Page 75614 of the Federal Register, Vol. 76, no. 232 issued Friday, December 2, 2011. http://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

FREQUENTLY ASKED QUESTIONS AND FEDERAL PRIVACY RESOURCES

FAQ: What is "directory information?"

FERPA permits very general information – so-called "directory information" – about students to be shared without student consent. This information includes their name, address, phone number and email address, dates of attendance, degrees awarded, enrollment status and major field of study. Institutions must notify students that the release of this information is permitted and provide them with an opportunity to opt out of having their directory information shared. This directory information does not include information on student behavior or academic outcomes, however, and may be of little or no use in evaluating the effectiveness of afterschool programs.

FAQ: What are "reasonable methods" to protect educational data?

FERPA requires that education agencies take all "reasonable methods" to ensure that student information is protected and used by its agents only for specifically authorized purposes. The U.S. Department of Education declined to define these purposes exactly, but provided a list of best practices in Appendix A of the December 2011 rulemaking. These practices include obtaining assurances against redisclosure, setting clear expectations around data destruction, maintaining a right to audit, verifying the existence of a data security plan, and ensuring the existence of a data stewardship plan (clear internal policies and procedures).

Further Privacy Resources:

- **Privacy and Technical Assistance Center (PTAC)**

  In April 2011, the U.S. Department of Education hired its first chief privacy officer (CPO), Kathleen Styles. The CPO heads PTAC, which offers a growing selection of technical papers and webinars on data privacy and security matters at http://www2.ed.gov/ptac.

- **Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records**

  This technical brief from PTAC describes the basic concepts and legal framework governing the release of student information. Several model memoranda of understanding are available through the U.S. Department of Education website at http://www2.ed.gov/about/offices/list/ovae/pi/cte/uiferpa.html.

- **Legal Issues in the Use of Electronic Data Systems for Social Science Research**

  Professor John Petrila of the University of South Florida provides an excellent overview of the laws and legal issues involved in sharing and using individual information, with an emphasis on research uses. Further information is available through the Intelligence for Social Policy project underway at the University of Pennsylvania at http://www.ispc.upenn.edu/.

SECURITY

Security is the enforcement of a privacy agreement. The assurances made to students, parents, and data partners that their confidentiality will be protected are only as credible as the ability of the coordinating entity to enforce them, and the trust between local partners can be permanently broken by negligence, malfeasance or the unauthorized redisclosure of private information. Management information systems present a new set of risks, in this regard, but also provide a set of tools for managing these risks.

Negligence is at the root of most security breaches. For example, in late 2011, the Wakulla County School District in Florida accidentally published the FCAT scores and Social Security numbers of 2,400 students to an open web server. Parents discovered the problem when one of them used Google to search for their child's name. In another recent incident, boxes filled with student information, including applications for free and reduced price school meals that contained financial information, were left in the garbage by a cleaning crew at an elementary schools in Santa Maria, Calif. It is not uncommon for laptop computers and thumb drives filled with unencrypted student files to go missing.

Malfeasance and the deliberate redisclosure of private information present further risks for a coordinating entity to manage. Website and network hacking attempts are frequently opportunistic attempts to exploit badly maintained technology, but MI systems may also be deliberately targeted. Last year, students hacked a school district's administrative record system in Blairsville, Pa., and downloaded teachers' addresses, salaries and Social Security numbers. Furthermore, deliberate redisclosure of student information by staff or any "authorized representative" of an education agency is a serious breach of the law that will be investigated by the U.S. Department of Education's Family Policy Compliance Office (FPCO). A finding by FPCO that a researcher or city coordinating entity working with the schools redisclosed student information in violation of FERPA carries at least a five-year ban on the receipt of any further private student data. If a compliance manager with access to the MI system were to share individual student academic information with providers without having received permission from parents, for example, the resulting FPCO enforcement could forbid the schools from sharing information with the coordinating entity for half a decade.

To avoid these problems and protect the city's and coordinating entity's reputations, city leaders often provide the following safeguards:

Create a Security Policy and Implement Internal Controls

City coordinating entities often begin by taking an inventory of all of the sensitive and private information that is, or will be, stored and processed by the organization. Providing ongoing training to staff will make them aware of what can and cannot be shared with whom and under what circumstances. Cities must also implement policies to reduce or eliminate negligence, such as ensuring that any student data emailed or kept on personal computers is encrypted. Finally, it is important to develop a protocol for handling breaches. This protocol should include clear guidance on how to identify the problem, who to inform,

and what information to share. This security policy should be periodically reviewed by the organization's board or data governance committee.

Further resources on data security include:

- *Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records*, a publication of the National Center for Education Statistics that is available at http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602
- The Data Security Policy of the United Way of Greater Rochester (N.Y.), which is available online at www.nlc.org/afterschoolmis

SECURE EMAIL AND FILE TRANSFER

System administrators often need to download, manipulate and distribute participant information for a variety of reasons: at the request of a program manager, to verify the completeness and accuracy of provider information, to develop grant proposals, or to report to funders. These spreadsheets – which may contain sensitive or confidential information – are sent in the clear (i.e., not encrypted) to colleagues and forwarded according to the discretion of the recipient(s).

There are at least two solutions to this problem:

- First, consider using secure email. Elizabeth Ramsay Marchese, manager of quality assurance for the United Way of Greater Rochester, suggests using a security tool that encrypts the entire email message and any attachments and prevents any third party from intercepting or later accessing the contents of the email.
- Encrypt the data file before transferring it. When the Jacksonville Children's Commission requests student information from Duval County Public Schools, SAMIS Senior Manager Juan Ruiz encrypts and emails a spreadsheet of all of the student participants for which the commission is seeking information to his colleagues at the district. The document returned by the district is also encrypted. One freely available file encryption tool is the PGP algorithm available through www.openpgp.org.

Youth information is much more secure in a management information system than it is on a computer desktop, on a flash drive, or attached to an email. Encrypting these data when it is away from "home" is a best practice.

Require Security Assurances from all MI System Vendors

The first threshold for any MI system is whether it can provide different levels of access to information to different system users: administrators, agency heads, program managers, and site staff. The configuration of these "role-based" permissions will be slightly different in every organization. However, it is crucial that the permission levels are carefully defined and that the vendor can accommodate them. Vendors should provide evidence that their system is secure from electronic attack, including information on the facility that hosts their servers and

the most recent audit of their security systems. Ideally, all data hosted by the MIS would be encrypted not only in transit – between the web server and the web browser – but also when it is "at rest" on disk. Finally, the vendor should provide a disaster recovery policy that outlines its procedures with regard to data breaches, application failures, and natural disasters.

Audit

Schools and other organizations that agree to provide information to a citywide afterschool system may request that one or both of the coordinating entity and its MIS vendor undergo a security audit. If not, the city or the coordinating entity should consider contracting for this service anyway. The audit should include a review of the organization's internal controls (its security policy). It should also, ideally, include two types of penetration testing: one attempt to hack the database from outside of the network and a second attempt using a guest account to "escalate privileges" and access information outside the scope of that user role. Reputable MI system providers are extremely security conscious and they should welcome this scrutiny.

Chambers of commerce and local nonprofits such as the United Way may be able to provide a recommendation for a good network security firm, many of which are regional. Credentials are not a guarantee of quality, but the number and proportion of the firm's employees certified as Information Systems Security Professionals can be an indicator of quality. More important is the standard the firm will use to evaluate an organization's security precautions and whether they have expertise in the privacy and security laws relevant to your data (such as FERPA). The Privacy and Technical Assistance Center's (PTAC) Data Security Checklist can be a helpful resource for developing a data security plan and is available at http://www2.ed.gov/policy/gen/guid/ptac/checklist.html.

"A tremendous amount of protected student information changes hands now, passed directly between teachers, principals and program officers informally, and stored in a variety of electronic and physical settings without much thought to security."

In a final analysis, the growth of student data systems – and out-of-school time MI systems among them – is likely to protect student privacy more than endanger it. A tremendous amount of protected student information changes hands now, passed directly between teachers, principals and program officers informally, and stored in a variety of electronic and physical settings without much thought to security. Teachers and afterschool program managers have every reason to share information on the youth they both serve. Data security is a major concern to schools, however, as many districts ratchet down their control over student information and replace these "ad hoc" teacher-provider relationships with formal agreements that meet the standard of federal and state privacy laws.

CITY EXAMPLE:

GOVERNING AND USING DATA IN GRAND RAPIDS

Believe2Become (B2B) is a place-based strategy in Grand Rapids, Mich., to close the achievement gap for 15,000 young people that live in four relatively disadvantaged areas of the city, dubbed "hope zones" (for more information, visit http://www.believe2become.org/).

Two years ago, the DeVos Foundation piloted a management information system provided by nFocus to support the initiative's summer learning programs. nFocus' KidTrax system helps to facilitate information exchange between the schools and community-based providers and provides a rich set of data on program participation and academic outcomes for evaluators (see page 32 for information on the B2B initiative's systems architecture).

To keep the providers, the MIS vendor, the local data partner, public schools and the third-party evaluators on the same page, the DeVos Foundation's research director, Edwin Hernandez, oversees no fewer than three working groups, which meet weekly or bi-weekly:

- A school-based committee that includes representatives from the Grand Rapids Public Schools (GPRS) and the Community Research Institute (CRI), the local data partner that links and de-identifies GPRS data for use by the B2B initiative and members of the evaluation team.
- An evaluation committee that includes CRI and the initiative's third-party evaluators.
- A management information committee that includes foundation staff, the MIS vendor (nFocus), and CRI, and that troubleshoots technical and provider issues. The DeVos Foundation is also encouraging the development of an MIS users peer group.

The number, structure and composition of data governance groups will vary according to the partners at the table in each community and the specific goals of the afterschool initiative. The example of Grand Rapids provides what Dr. Hernandez understatedly describes as a "robust" approach to managing these informational tasks.

[6] Security standards include the National Institute of Standards and Technology (NIST) guidelines, the International Standards Organization's (ISO) 27001 framework on Information Security Management, and the National Security Agency's (NSA) Information Assurance Directorate.