WEBINAR SUMMARY

Confidentiality Issues: Addressing Questions about Sharing Data among Organizations

April 2014

elcta

Early Learning Challenge Technical Assistance

Many people have questions about the sharing of data about children, such as the inputting of developmental screening results and other sensitive child-level data into a statewide database. Questions about confidentiality issues are commonly asked of the Privacy Technical Assistance Center (PTAC); the ELC TA program; and the Center for IDEA Early Childhood Data Systems (DaSy Center), which focuses on parts B and C of the Individuals with Disabilities Education Act (IDEA).

How do privacy implications impact organizations and the decisions they make? While the answer is often the unpopular "It depends on the specific case," there are several key points that people can consider when storing, providing access to, and conducting analyses on data covered by the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA). This document describes these key points and also provides answers to common questions and questions asked at the webinar. If your needs go beyond the answers that appear here, please direct specific questions to your local technical assistance center.

KEY POINTS ON SHARING DATA COVERED BY FERPA AND HIPAA

Seven key points to know with regard to the federal laws on sharing education and health data—with a special emphasis on data obtained and used by early childhood education programs—are presented concisely here. The laws are complex, but keeping these points in mind will help states and agencies begin to navigate the legal landscape as they develop and enhance their early childhood data systems.

1. Properly de-identified data can be shared. Under both FERPA and HIPAA, if the data have been properly de-identified, they can be shared. This should be the first choice for sharing data for research or other purposes, as it limits the risk of unauthorized disclosure of personally identifiable information (PII). It is important to understand that properly de-identifying data involves more than simply removing names and Social Security numbers. For example, data on small subgroups may present a problem, while aggregate data may not.

2. To share PII, get consent. In most cases, consent is the recommended approach for sharing PII with nonprofit organizations and other third parties. This is commonly also the easiest option for all involved.

The ELC TA Program provides and facilitates responsive, timely, and high-quality technical assistance that supports each Race to the Top–Early Learning Challenge (RTT-ELC) grantee's implementation of its RTT-ELC projects.

ELC TA is administered by AEM Corp. in partnership with ICF International.

For more information, visit https://elc.grads360.org

This ELC TA resource is based on a webinar held on April 21, 2014, sponsored by ELC TA.

Webinar Presenter:
Baron Rodriguez
Privacy Technical Assistance Center (PTAC) Director, AEM Corporation

Moderator:
Kathy Thornburg
ELC TA Specialist

The Early Learning Challenge Technical Assistance (ELC TA) program is run through a contract from the U.S. Department of Education in partnership with the U.S. Department of Health and Human Services' Administration for Children and Families. The content in this resource does not necessarily reflect the position or policy of the U.S. Department of Education or the U.S. Department of Health and Human Services, nor does mention or visual representation of trade names, commercial products, or organizations imply endorsement by the federal government.

3. Directory information is administered by local education agencies (LEAs). Under FERPA, LEAs control their own directory information. If a large entity such as a state wishes to access directory information, it must obtain permission from every district to which the information pertains. Also, while there are provisions that allow parents to opt out—thus preventing their children's information from appearing in yearbooks, handbooks, rosters sent to parents, and so on—these children's directory information can still be shared with school officials and for purposes of audit and evaluation of the program.

4. FERPA protects education records. Determining *when* something is an education record is not always easy to do. For instance, people often wonder whether emails, videos, and text messages—all commonly used in early childhood settings—qualify as education records. Often, the determination is made based on what specifically was sent, and for what purpose. In other words, context and data flow matter.

5. FERPA does not focus on how to protect data. Instead, it focuses on who has access to data and for what purpose. People commonly ask whether a particular data security system or protocol is adequate under FERPA, but the law is broad in this area, stating that "reasonable methods" must be used to protect data. If an organization is compliant in data security under HIPAA—which is more prescriptive in this area—it is generally compliant under FERPA.

6. Only governmentally funded education programs are subject to FERPA. Education programs that are fully funded by nonprofit organizations, including religious and nonreligious organizations, need not comply with FERPA. However, in general, if any federal dollars are given to and used by a program, the program must comply with FERPA. This includes state dollars that are administered by the U.S. Department of Education. If a program uses only state and/or local funds that are not administered by the Department, it most likely does not need to comply with FERPA, although it is still a best practice to do so.

7. The definition of an "education program" is broad. FERPA defines "education program" to include a wide variety of programs, including a wide variety of early childhood programs—even programs that do not reside at an education agency. For example, a program could be housed and administered by a health agency and still be classified as an education program under FERPA.

Definition of "Early Childhood Education Program" from 20 U.S.C. 1003(8)

"The term 'early childhood education program' means—

(A) a Head Start program or an Early Head Start program carried out under the Head Start Act (42 U.S.C. 9831 et seq.), including a migrant or seasonal Head Start program, an Indian Head Start program, or a Head Start program or an Early Head Start program that also receives State funding;

(B) a State licensed or regulated child care program; or

(C) a program that—

(i) serves children from birth through age six that addresses the children's cognitive (including language, early literacy, and early mathematics), social, emotional, and physical development; and

(ii) is—

(I) a State prekindergarten program;

(II) a program authorized under section 619 [20 U.S.C. 1419] or part C of the Individuals with Disabilities Education Act [20 U.S.C. 1431 et seq.]; or

(III) a program operated by a local educational agency."

COMMON QUESTIONS AND ANSWERS

This section lists common questions about early learning confidentiality issues and their answers.

Who is allowed to view record-level child data, and under what circumstances?

Generally, FERPA requires prior written consent before PII from education records can be disclosed to a third party. However, there are exceptions to the consent requirement. FERPA's audit and evaluation exception provides one mechanism for linking education data to wage data (or to other agency data) without consent. (Note that the term "audit" means program evaluation.) Refer to the federal definition of the term "early childhood education program" (shown on the previous page) to determine whether a particular early childhood program's records are classified as education records under FERPA.

When is prior consent required for the disclosure of information?

FERPA provides some exceptions to the requirement of prior consent. These include the following:

- Directory information
- Use by school officials
- Studies
- Audits and evaluations
- Health and safety emergencies
- Other purposes as specified in section 99.31

There is no research exception. Therefore, to share data for research, one must either obtain a de-identifiable dataset, or, if the dataset is identifiable, it must fall under one of the exceptions listed above, such as the audits and evaluations, school officials, or studies exception. To fit under the studies exception, the study must "improve instruction," and it must be "for or on behalf of a local education agency," which generally prevents the studies exception from being used at the state level.

The school officials exception allows LEAs and schools to use data for necessary purposes. The school officials exception can be used to disclose records to a third party if all of the following conditions apply:

1. *The third party performs a service or function for which the LEA or school would otherwise use its own employees.* This specification allows the LEA or school to outsource work to partner organizations and individuals, as needed.
2. *The third party is under the direct control of the LEA or school with regard to the use and maintenance of the education records.* In this context, "direct control" does not mean that the LEA or school controls the third party, but that the LEA or school has the final say on how the data are used.
3. *The third party's function is as a school official with a legitimate educational interest, and this is specified in an annual notification of rights to parents.* FERPA requires that parents be notified annually about which partners and volunteers have access—due to a legitimate educational interest—to their child's data.

What resources support the planning and development of policies on including developmental screenings in an early childhood integrated data system (ECIDS), a statewide longitudinal data system (SLDS), or any permissions-based portal?

One great place to access resources about including data in an ECIDS, an SLDS, or any kind of permissions-based portal is the PTAC Toolkit webpage, located at *http://ptac.ed.gov/toolkit*. On this page, you will find resources such as issue briefs; checklists that describe how to put together a data sharing agreement, how to partner with others to share data lawfully under FERPA, how to respond to a

data breach, and so on; FAQs; case studies; webinars; and more. More resources will be added soon to the PTAC Toolkit, so check the website regularly to obtain up-to-date information.

In addition, local technical assistance centers can provide answers to specific questions, as well as assistance in mapping data flow and designing systems.

How might a state get started on this, who should be involved, and are there examples from other states?

A recent meeting in San Diego brought together people from six state teams who were getting started in addressing confidentiality issues and creating data systems. Included were state SLDS directors, partners in early childhood education, attorneys, data directors from parts B and C of IDEA, and representatives from early childhood organizations. The purpose of the meeting was to get everyone on the same page, map out how to connect the data and how to collaborate in doing so, and address and overcome the legal hurdles.

A state or agency can gather people together to accomplish similar things. Following the four-step process shown in figure 1 and explained below will help a team meet its goals efficiently.

1. First, look at what types of data are being integrated, determine which agencies need to be involved, and involve these agencies very early in the conversation.
2. Then, identify specifically which data types will be shared—especially which PII will be shared.
3. Once a team has inventoried who is involved and which data are needed, it should look at the applicable laws. Look at not only federal laws, but also state and local laws. At present, there are 33 bills in state legislatures relating to children's privacy and the security of education data, so staying abreast of current bills in the relevant state legislature is vital. Also note that being compliant with HIPAA and FERPA represents a relatively low bar, and the bar can and should be set higher by doing additional things to protect the data and be transparent about their use.
4. Finally, map the data flow in a visual format. Map out where the information resides, where it will go, and what the output of the combined data will be. A visual map of the data flow is essential because it will reveal any holes in data linking and data protection that need to be filled, and it will sort out issues of ownership, accountability, and the collection of data.

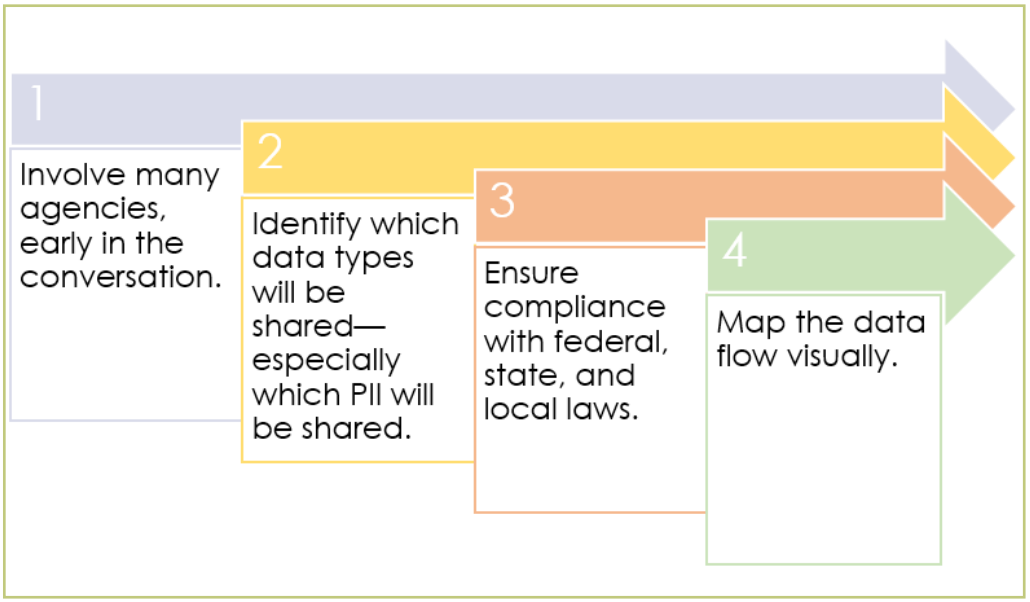

Figure 1. The process for getting started in creating a compliant system for data sharing

The key to accomplishing this process is to take baby steps while proceeding in the correct order (shown in figure 1). PTAC and local TA centers can provide assistance with this process.

LIVE QUESTIONS AND ANSWERS

This section lists the questions asked during the live webinar and the answers given.

Q: Has PTAC been involving health providers such as pediatricians in the discussion about data sharing and confidentiality as pertaining to developmental screenings?

A: We (PTAC) have included agencies representing the interests of health providers, though not health providers themselves. These agencies are involved in consolidating data from developmental screenings into education records. One issue we are working on is that, as developmental screening data are integrated into education records, they move from being governed by HIPAA to being governed by FERPA. We are working on determining when that happens and who needs to be involved in the process.

Q: What issues surround data security as it relates to the Heartbleed bug?

A: PTAC has written an issue brief on the Heartbleed bug, which is available at *http://ptac.ed.gov/document/surviving-heartbleed-guide*. Heartbleed is not a virus or malware; it is a vulnerability built into OpenSSL, which is popular software that protects the security of websites. (When a URL begins with *https://*, this indicates that the webpage is protected by security software.) Due to the Heartbleed vulnerability, attackers can peer into a computer's memory and possibly retrieve encryption keys. Software patches to fix the problem are now available, and businesses, organizations, and individuals are installing them on their websites. There are also plug-ins for browsers that detect the vulnerability of specific sites. Many questions still surround the Heartbleed bug, especially regarding how big the exploitation has been, since the vulnerability existed for two years before being discovered and made public this month. For more information, please visit *www.heartbleed.com* and *www.openssl.org*.

Q: We are working on our quality rating and improvement system (QRIS), which is being created with federal and state government funds and is authorized by the state code. Our QRIS is not managed by our LEA system, but by a nonprofit management partner, which also employs technical assistants who function as instructional leaders. We will be requesting parent consent for formative assessment. How might the technical assistants from our nonprofit management partner access student-level information so as to assist teachers and site-based educational leaders in analyzing information and then using this data analysis to develop and improve instructional practices?

A: It sounds like your situation will fall under the definition of an education program. Some QRISs do not link to student-level information, but it sounds like yours does. That being the case, to share data you must either get consent or use one of the exceptions. If you use the school officials exception, you will need to notify parents about what the data will be used for. However, it sounds like you are obtaining parent consent, and therefore, you will notify parents in a consent form about the purpose and recipients of the data sharing. There are three requirements for a consent form. It must say (1) what data about the child will be shared, (2) with whom, and (3) for what purpose. These three elements must be described specifically and clearly. For example, you must list out each type of data (e.g., name, date of birth, etc.) that will be shared. Then, parents will need to opt in for the data to be shared.

Q: For about how long should an early childhood formative assessment record be available into the child's school years, so that teachers can see a child's records going back to preschool?

A: The easiest way to share data forward is to build this type of data sharing into a parent consent form. If the data will be shared through one of the FERPA exceptions instead of through a consent form, then you must state in the annual notification to parents that information will be shared with the elementary school or the kindergarten teacher for the purpose of preparing the teacher to instruct the student at the new facility.

A representative from California shared that this state requires contractors to save assessment data for five years after a child leaves a program, although the data are probably useful to teachers for only a couple of years. FERPA is fairly silent on the retention of records. However, the longer you keep data in your system, and the more data you keep, the higher is the risk for unauthorized disclosure. So we recommend that you practice data minimization. It's a best practice to follow the archival rules established by your state.

Q: What methods of data sharing across sectors do PTAC representatives see people using (for example, statewide registries, health information exchanges, etc.)?

A: At PTAC, we see a wide variety of methods of data sharing, and these are different in different places across the U.S. The methods used depend on what data people are trying to share and who is partnering in the sharing. SLDS is one key partner helping to facilitate the exchange of data. Often, we see the sharing of individual records (records that are not aggregated) for transactional purposes. In this case, data are sent to a receiver for one specific purpose, and the data are not used for any other purpose. In the case that people wish data to be used for dual purposes—for example, for improving instruction *and* for enrolling children—it can be more challenging to comply with FERPA because different data purposes are treated differently under the law.

Q: Does information become an education record when an early intervention referral is made, or not until the LEA is able to connect with the family and obtain consent? Can we share information back to a health care provider about the status of the referral and which LEA they can contact to get more information?

A: The answer depends on which information was shared and the specific circumstances of the sharing. Because there are so many variables, we cannot give a precise answer here. This is an excellent question for you to ask PTAC or your local TA center. We will have a call with you to discuss your situation in detail and answer it fully. Please contact us—that's why we're here!

Q: To what extent are the records of children enrolled in licensed (private) child care programs subject to the requirements of FERPA?

A: These programs are early childhood education programs according to the federal definition, but the records of children enrolled in them are not subject to FERPA unless federal funding is being received by the programs. These programs' records may, however, be subject to HIPAA if they include health information.

Q: How should we handle emailing child information, such as Individualized Education Programs (IEPs) and Individualized Family Service Plans (IFSPs), to places such as child care centers and family child care locations?

A: IEPs and IFSPs are part of the education record and should be transmitted securely. Visit the Security Best Practices section of the PTAC Toolkit webpage (*http://ptac.ed.gov/toolkit*) to access

detailed information on identity authentication, secure methods of transmitting information electronically, and more. It is important to verify that you are sending information to the right person. A common and dangerous mistake is to send information to someone with the same first name but a different last name. It is also important to verify that the information was received. One good practice is to encrypt your files as attachments and protect them with a password. The resources on our website explain in detail how to do these things and more. See also the Office of Special Education Programs' letter to Ms. Breton on March 21, 2014, located at *https://www2.ed.gov/policy/speced/guid/idea/memosdcltrs/acc-14-000862r-me-breton-email-3-21-14.pdf*.

RESOURCES

The Heartbleed Bug
www.heartbleed.com

Office of Special Education Programs' letter to Ms. Breton on March 21, 2014
https://www2.ed.gov/policy/speced/guid/idea/memosdcltrs/acc-14-000862r-me-breton-email-3-21-14.pdf

OpenSSL
www.openssl.org

PTAC Help Desk
PrivacyTA@ed.gov
855-249-3072

PTAC Toolkit
http://ptac.ed.gov/toolkit

Recording of the Webinar
http://elcta.adobeconnect.com/p1edj1nj2hj/

Surviving Heartbleed Guide
http://ptac.ed.gov/document/surviving-heartbleed-guide