Comments of the World Privacy Forum

Regarding the U.S. Department of Education Notice of Proposed Rulemaking for the Family Educational Rights and Privacy Act, RIN 1880-AA86, Docket ED-2011-OM-0002-0001

Submitted via http://www.regulations.gov and via email to FERPA@ed.gov

Regina Miles
U.S. Department of Education,
400 Maryland Avenue, SW.,
Washington, DC 20202.

May 23, 2011

The World Privacy Forum appreciates the opportunity to comment on the Department's proposed rule change to the Family Educational Rights and Privacy Act at 76 Federal Register 19726 (April 8, 2011), http://www.federalregister.gov/articles/2011/04/08/2011-8205/family-educational-rights-and-privacy. The World Privacy Forum is a non-partisan, non-profit public interest research and consumer education organization. Our focus is on conducting in-depth research and analysis of privacy issues, in particular issues related to information privacy. More information about the activities of the World Privacy Forum is available at <http://www.worldprivacyforum.org>.

In general, we find the Department's proposed changes to FERPA troubling on a number of grounds. Most significantly, we believe that the Department does not have the legal authority to make all of the changes to the privacy requirements in FERPA that it proposes. We also have strong concerns that the increased sharing of student information that the proposed rule will allow will diminish student privacy in a major and permanent way. WPF does support one proposed change to FERPA, which we discuss in the comments.

I. Department Authority

We seriously doubt the Department has legal authority to weaken or even change the privacy requirements in FERPA in all the ways that it proposes. 20 U.S.C. 9871(e)(2)(C)(i) provides:

> Each State that receives a grant under subsection (c)(2) [for statewide P–16 education data systems] shall implement measures to—

(I) ensure that the statewide P–16 education data system meets the requirements of section 1232g of this title (commonly known as the Family Educational Rights and Privacy Act of 1974);

This language makes it clear that the law expressly contemplated application of the existing law and its rules. In passing the American Recovery and Reinvestment Act of 2009 (ARRA), Congress did not amend the preexisting requirement in the America COMPETES Act that requires states developing statewide longitudinal data systems (SLDS) to comply with FERPA. Nor did the ARRA direct the Department to amend the rules to conform to the new requirements. Were there a conflict or significant problem with the existing FERPA regulations, Congress could easily have called for a change or a review. The absence of any such directions in the law leaves the Department without authority to make changes and certainly without any authority to weaken the privacy requirements already in place. In our view, Congress wanted the new data systems to meet existing FERPA standards.

Further, nothing in ARRA's appropriation of funds for statewide data systems directs, contemplates, or even hints at a change in the FERPA regulation or in existing law quoted above that requires states to comply with FERPA. It is an appropriation and not legislation. We also observe that if any of these other statutes directed or even suggested changes to the FERPA rule, then the authority citation for the changes would have included these other statutes and not just cite to FERPA. The absence of additional citations may be telling.

We note further that the Department declined to make changes to FERPA regulations for SLDS when it changed the FERPA regulations in 2008 The Department said expressly that it was "without authority" to exempt data sharing as requested by those who commented on the previous NPRM. Nothing in ARRA gives the Department authority to do what it said earlier that it had no authority to do. Yet the current NPRM is replete with examples where the Department now proposes to allow activities that it heretofore determined were not permitted, and the only real reason for the change is expedience. If the Department wants to allow additional uses of confidential student records, it should go back to the Congress and ask for the authority. We believe that the Department is well aware of that the legal grounds for changes to FERPA regulations are shaky at best and non-existent at worst. The best outcome here would be a public debate over the proper balance between privacy and the substantive educational objectives, and the right place for that debate is the Congress.

The effect of many of the changes that the Department proposes will be to allow for the disclosure of heretofore confidential student records to agencies, organizations, and private entities that have little to do with education. It is inevitable that this allows the records to be used for secondary purposes, something that FERPA was largely intended to prevent. The result will be that student records will become general input to a wide range of activities, studies, evaluations, and the like on the pretext that there is some education result to be derived eventually. Student and parental records will be scattered to the winds to remote and untraceable parties, used improperly, maintained with insufficient security, and become fodder for marketers, hackers, and criminals. The confidentiality that FERPA promised to students and their families will be lost.

The Department relies on the fiction that vague purpose tests and unenforceable written agreements will provide protections. What the Department is essentially creating is a free-for-all with student data, which will be passed around from one organization to another, used improperly, exposed to the world, or lost. We remind the Department that students are not the only people at risk. Schools may have significant information, including health and financial information, about parents. This information is threatened just as much as student information.

In the longer run, the lack of any remedies for aggrieved individuals under FERPA may result in a burst of legal creativity, as students and parents affected by misuse and lack of security seek remedies. The lack of remedies for aggrieved students and families under FERPA may not protect anyone when data is shared beyond the scope of FERPA or to new entities that are subject to and protected by FERPA's peculiar and limited enforcement scheme. The cost of litigation and the payment of damages could become a burden to schools, states, and others who are responsible. Courts and state legislatures will find it necessary to impose new limits because the Department refused to take the appropriate steps here. It will only take one scandal to produce new restrictions and real sanctions.

If the Department wants to accomplish the objectives reflected in the proposed regulation, it needs clear statutory authority. It should ask the Congress to amend the law so that any new regulation will have a firm basis in law and so that there is an opportunity for public debate over the proper use of student records for secondary purposes.

II. Authorized Representative and Written Agreements

The Department proposes to define the term *authorized representative*. Since this is a term in the current rule, we do not dispute the Department's authority to offer a reasonable definition. However, the proposal highlights an already existing enforcement shortcoming of FERPA. The NPRM states:

> Specifically, we would provide, in proposed § 99.35(a)(2), that responsibility remains with the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) to use reasonable methods to ensure that any entity designated as its authorized representative remains compliant with FERPA. We are not proposing to define ''reasonable methods'' in the proposed regulations in order to provide flexibility for a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) to make these determinations. However, we are interested in receiving comments on what would be considered reasonable methods.

As FERPA information increasingly spreads downstream to third party, fourth party, and even more remote organizations that have not been subject to direct enforcement by the Department, the hope of maintaining compliance with FERPA rapidly approaches zero. We discuss enforcement problems later in these comments.

The Department's objective of having reasonable methods that will "ensure" compliance with FERPA sounds worthy, but there are no such methods. We expressly object to the use of the

word "ensure" because it is unrealistic and misleading. The best the Department can hope for is a method that will provide some incentive to comply.

The proposed change will not accomplish much if it relies mostly on non-binding suggestions. We observe that even severe criminal, civil, and administrative penalties (even with some recent, actual, and aggressive administrative enforcement) have not provided sufficient incentive to "ensure" an end to security and privacy breaches by health care institutions and their business associates subject to HIPAA health privacy and security rules. We object to the suggestion that the Department will issue *non-regulatory guidance* for this purpose. The regulation can and should do better, and the Department should impose binding requirements.

A. Elements that should be included in the required written agreements

Since the Department is already proposing to specify elements of the written agreements, it can certainly specify enforcement and oversight mechanisms that will accomplish more than can be hoped for from *non-regulatory guidance*. We offer the following suggestions for provisions that should be expressly mandated in the written agreements that the Department proposes to require in §99.35(a)(3).

1. Consent. An existing mechanism allows for all of the disclosures that the Department contemplates without changing any regulation. *Parental consent* can support all disclosures, direct or otherwise. If parents view the purposes of a disclosure as worthwhile, consent will be obtainable. It may be more cumbersome than simply eliminating a requirement for consent by conveniently issuing a regulation. Nevertheless, consent is a method that will vastly increase parental involvement, local awareness of data activities, and accountability. The value of these objectives outweighs the difficulty of relying on parental consent.

2. Liquidated damages. The written agreements should be required to include a provision calling for liquidated damages to be paid by an authorized representative to the institution that originally disclosed the information. We suggest that the amount of damages be: a) a percentage of revenues (25% might provide a sufficient incentive) paid by the authorized representative; or b) not be less than $100 for each record used or disclosed in violation of FERPA. Any damages collected could be kept by the institution or distributed to the data subjects whose privacy was violated.

3. Third party beneficiary. Any written agreement should be required to make students and parents third party beneficiaries of the agreement. The goal is to allow any individual aggrieved by a violation of the confidentiality obligations to sue the authorized representative to recover damages if lawsuits are allowed under state law. This requirement would provide a useful remedy that would allow for private enforcement against authorized representatives (and not against innocent educational institutions).

4. Transparency. Any person seeking to become an authorized representative should be required, under penalty of perjury, to disclose to an educational institution and to the public whether the person has violated or been accused of violating any written agreement that involved the disclosure of data subject to FERPA.

5. Breach Notification. We observe that there have been reported breaches of student records, and there will certainly be more.[1] The Department needs to address who will take responsibility if no state or federal breach notification law applies. If data transferred to an authorized representative is not subject to a state or federal security breach notification law, the written agreement should provide that the authorized representative must provide breach notices to data subjects comparable to those generally required under state laws. Each written agreement should also provide expressly that an authorized representative responsible for a breach will bear the cost of breach notices. A mandatory provision on breach notification will avoid finger pointing and litigation when the issue arises, as it surely will.

6. Audit. Every written agreement should require an annual independent third-party audit of the authorized representative's privacy and security policies and practices. The results of the audit should be publicly disclosed.

B. Other suggestions

First, we are concerned that the current provision is not express enough about data destruction. We recommend that written agreements must have some fixed period for data destruction. Allowing data to be retained forever is an invitation to mischief or worse. We suggest an absolute time limit of five years. If there is a need for data after a fixed period, the parties can revisit the issue and revise the agreement.

Second, we suggest that all written agreements must be public documents either in whole or in part. The purpose is to allow for public oversight of data disclosures without protracted fights over access to records. We doubt that any of these agreements will contain proprietary or other information that would justify withholding, but we would not object if the Department chose to allow for the possibility.

Third, we suggest that anyone entering into a written agreement must specify in the agreement the legal authority for the disclosure. The goal is to ensure that anyone disclosing data must be

[1] See, e.g., *Student Records Found Dumped in Trash Bins* (March 2011), http://www.myfoxny.com/dpp/news/student-records-found-dumped-in-trash-bins-20110328; *Hackers may have accessed thousands of SC students' information* (April 2011), http://www.live5news.com/story/14468839/hackers-may-have-accessed-thousands-of-students-information; *COTC students' personal information left unsecured* (April 2011), http://www.newarkadvocate.com/article/20110419/NEWS01/104190308; *1 stolen Albright laptop found; 1 still missing* (April 2011), http://readingeagle.com/article.aspx?id=301685; *More Student SSNs Were at Risk*, TEA Says (April 2011), http://www.texastribune.org/texas-education/public-education/more-student-ssns-were-at-risk-tea-says/.

sure that it has legal authority to do so. Including the information in a public agreement will also facilitate public oversight of the activity.

III. Implied Authority

On page 19731 of the Federal Register, we find this paragraph:

> In the event that an educational agency or institution objects to the redisclosure of PII it has provided, the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) may rely instead on any independent authority it has to further disclose the information on behalf of the agency or institution. The Department recognizes that this authority may be implied and need not be explicitly granted.

This language tells a state or local authority that it can ignore any school that objects to disclosure of PII it provided to the authority and disclose that school's data anyway. The authority does not even need specific statutory authority to override a school's express objections. Apparently, the Department's view is that anything goes unless it is expressly prohibited by law.

In effect, the Department is saying that it has no intention of enforcing any confidentiality rules that are violated in furtherance of an activity that the Department approves of. There has been precious little enforcement of FERPA to begin with, but this statement essentially guaranteeing that there will be no confidentiality enforcement even for sharing of data done without any legal authority and over the objection of the originating school is shocking. The Department is inviting battles between schools and state authorities over control of student data, and the Department is prejudging that whatever the state authorities want to do is always the right thing. It will surely come back to haunt the Department as states interpret it to mean that anything goes when it comes to sharing student records.

IV. Family Policy Compliance Office Enforcement

The revised § 9935(d) would read:

> (d) If the Family Policy Compliance Office finds that a State or local educational authority, an agency headed by an official listed in § 99.31(a)(3), or an authorized representative of a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3), improperly rediscloses personally identifiable information from education records, the educational agency or institution from which the personally identifiable information originated may not allow the authorized representative, or the State or local educational authority or the agency headed by an official listed in § 99.31(a)(3), or both, access to personally identifiable information from education records for at least five years.

This enforcement provision is too narrow. First, it sanctions only the improper redisclosure of PII. Protecting privacy is more than preventing improper disclosures. There are other

inappropriate activities that affect privacy, including *using* records for an improper purpose; examining individual records without justification; not securing records properly; obtaining information by unfair or improper means; not maintaining records with appropriate accuracy, completeness, and timeliness; not specifying the purposes for which records may be used or disclosed; and not allowing access to or correction of records when appropriate. All of these privacy violations should be sanctionable, and the provision should be expressly revised to say so.

Second, the sanction proposed only prevents further disclosures by the educational agency or institution from which the personally identifiable information originated. If a person is found to have violated the rules under which data was obtained, the sanction should prevent that person from obtaining data from *any* educational agency or institution or from any authorized person. The sanction should apply across the board, and a violator should be banned from obtaining student records from any educational institution anywhere in the country. The sanction should apply broadly to subsidiaries and other entities controlled or working with the violator.

Third, we have already stated that the Department does not have the legal authority to authorize the disclosures in this NPRM. We doubt that the Department has the authority to expand the enforcement authority of the Family Policy Compliance Office to cover a third party who is not an educational agency or institution. As the Department well knows, its authority to enforce FERPA is severely limited by the statute. If the Department attempts to sanction anyone who is not an educational agency or institution, the existing denial-of-funds sanction may not be relevant or available.

It is quite likely that anyone the Department seeks to sanction will challenge its authority, and there is a good prospect that a challenge will succeed because the Department is expanding its traditional authority without any new statute that gives it the authority to do so. We could even end up in the worst of all cases, where the Department's authority to authorize new disclosures is not challenged, but its authority to enforce restrictions against some authorized data recipients is denied. The best solution to this problem is to seek an amendment to the statute.

V. Education Program

The proposed definition of *education program* is vitally important because it determines the realm of activities that may contribute and obtain data. The proposed standard – any program that is principally engaged in the provision of education – is far too vague. We do not know what *principally* means. Does education have to be 90% of a program's function? 75%? 51%? 10%? Who is responsible for making the determination? What information must a potential discloser obtain before it can be assured that it is making a lawful disclosure? Can it rely on a statement by a self-proclaimed education program that the program qualifies?

We also do not know what a *program* is. If a commercial website offers training in use of a web browser, would that website qualify? Would that website then be able to seek data on other students on the pretext of determining if its educational efforts are working? Would it matter if the website were owned by a large Internet company with multiple non-educational activities? Would an ad hoc program at a local library aimed at teaching people how to obtain a mortgage

qualify? Would a direct marketer who sells books that purportedly educate readers qualify? Would a neighborhood book club with a stated purpose of sharing knowledge about literature qualify? Does every Boy Scout or Girl Scout troop qualify? What about a summer camp with a batting clinic? Does a Sunday School qualify? Every day, we receive spam messages offering "job training" in a variety of technical skills. Would these seemingly fraudulent training programs also qualify? Could the marketers, hackers, or criminals that run some of these activities obtain information on millions of students to further their attempts to entice students to enroll in their questionable or illegal "educational program" activities? Would a job training program – legitimate or otherwise – located in another country qualify? Could a school share identifiable student data with an *educational program* in Iran or North Korea or in some jurisdiction where the data might be fodder for identify thieves? The proposed rule could be read to allow all of these disclosures and more

The Department needs to draw clearer and tighter lines here. The potential for wholly unwarranted disclosures to recipients who are well beyond any possible enforcement, penalty, or civil action is real and immediate. The Department must make it clear how determinations are to be made and who is to be accountable for those determinations.

VI. Limited Directory Information Policy

The NPRM proposes this change to the directory information provision:

> § 99.37 What conditions apply to disclosing directory information?
>
> (d) In its public notice to parents and eligible students in attendance at the agency or institution that is described in paragraph (a) of this section, an educational agency or institution may specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both. When an educational agency or institution specifies that disclosure of directory information will be limited to specific parties, for specific purposes, or both, the educational agency or institution must limit its directory information disclosures to those specified in its public notice that is described in paragraph (a) of this section.

The World Privacy Forum is pleased to support this change. Indeed, we proposed in our comments on the last round of FERPA regulation changes that there was a need to establish categories of directory information. See Comments of the World Privacy Forum regarding Notice of Proposed Rulemaking, Family Educational Rights and Privacy, 34 CFR Part 99, RIN 1855-AA05, Docket ID ED-2008-OPEPD-0002, May 6, 2008, http://www.worldprivacyforum.org/pdf/WPF_FERPAcomments052008fs.pdf. We reproduce our earlier comments here:

> Part of the difficulty here is the treatment of all types of directory information as the same. It is one thing to circulate a student list to parents in the school. It is something else to circulate a full list of every permissible element of directory information to the world outside the school. We suggest that the Department consider establishing categories of directory information.

> Some information would be eligible for circulation within the school community, while other information might be eligible for broader circulation. We worry that administrative convenience or regulatory uncertainty may result in schools putting more information into a public directory than is really needed.
>
> While we recognize that the statute allows student directories and that directories can serve useful purposes, a directory is still a major imposition on the privacy of a student and parent. This conclusion is even more important in this era of international identity theft activities than it was when FERPA first became law. The contents of a student directory should be based to some extent on the need-to-know principle.

We suggest that the proposed language be amended to make it expressly clear that a limited disclosure can cover only some rather than all directory information. We further suggest that the Department consider how a school might be able to enforce a disclosure of directory information for a limited purpose if a recipient uses the information for an unauthorized purpose. There is no apparent remedy under FERPA, and the Department might want to require schools making limited purpose disclosures to use written agreements for the disclosures and to use some of the enforcement and oversight elements we suggest above for written agreements.

VII. Other thoughts

A. Ban nationwide data systems

We have other suggestions that go beyond the NPRM and probably beyond the current authority of the Department. The idea follows from the creation, existence, and expansion of statewide longitudinal data systems. These systems will, regardless of the presence or absence of overt identifiers, will become data honey pots. The data will attract other users who have no specific interest in education but who do have an interest in finding data about students and their families. The uses will include, but not be limited to, the police, national security agencies, immigration law enforcers, private litigants, social welfare program, and others. Every database with personal information eventually attracts other users, and it is likely that the databases being created for educational use will be no different.

Statewide longitudinal data systems will attract other users. A nationwide data system will attract other users in large numbers. We do not know whether current plans include any type of nationwide system is contemplated. It would be appropriate for the Department to state expressly that it does not want and will not support any nationwide system of any type, whether a central repository or a central pointer system. A nationwide system would be a privacy disaster of unparalleled dimension, eventually becoming a central record system on every family and every individual in the United States.

B. Protect SLDS against secondary uses and legal process

We also suggest that the Department develop a legislative proposal that would protect each SLDS and any derivative databases from secondary use and from compelled disclosure to law enforcement and private litigants. A possible model for legislation is 13 U.S.C. § 9 covering census records. We cannot determine at this time whether the legislation should be enacted at the federal or state levels (or both), but a single uniform federal law would be the most efficient way to accomplish the goal. It might be helpful to allow state legislation to provide protections that exceed the federal floor. A model here would be the privacy legislation included in the Health Insurance Portability and Accountability Act.

We recommend that the Department study this suggestion outside of the NPRM process and make recommendations to the Congress on the best way to accomplish the purpose. This task should have a high priority because once secondary and tertiary users discover the utility of statewide (and ultimately nationwide) databases with information on every child, every household, and eventually every adult, those users will beat a path to its door.

C. Protect other national student data collections that pose privacy issues

We also note for the record that some large non-profit national educational standardized testing companies collect a great deal of personal and sensitive information from students as a voluntary adjunct to the exam process. For example, parental income, disability status, and much more can be part of the information requested from students. The exams may take place in school settings, but the data collection nevertheless appears to be outside of FERPA's reach. FERPA should be expanded to cover such data collections taking place on school grounds.

We note that this is the kind of data collection that can be readily combined with SLDS data. We also note that because the voluntary data collections are being requested as an adjunct to an exam that most students view as important to their academic future, that students will potentially be favorably biased towards releasing even very sensitive information that they would otherwise not be comfortable releasing. This favorable bias is, we believe, increased by testing that may occur on school grounds.

Respectfully submitted,

s/o

Pam Dixon
Executive Director,
World Privacy Forum
www.worldprivacyforum.org