Sheila Kaplan
347-486-0361
www.educationnewyork.com
sheila@educationnewyork.com

Education NEW YORK

Protecting Student Privacy in Research Projects

While a great deal of attention has been paid recently to protecting the privacy of students' personal information and education records, families and educators also need to be aware of the use and disclosure of students' personal information in research conducted by universities and other entities.

Many research activities are well-intentioned, and some produce useful results. However, the disclosure of student information to researchers exposes students to additional privacy risks. The researchers themselves have varying levels of knowledge related to the privacy and security of the information they collect, analyze, and, in many cases, publicize. For example, a researcher may use a laptop that is filled with identifiable student data that are part of a research project. How secure is that laptop or the Wi-Fi networks the researcher accesses?

Student records are accorded some privacy protections while the records are in the possession of their schools. For example, the Family Educational Rights and Privacy Act, or FERPA, provides some privacy protections to students' education records, but the law does allow *non-consensual* (without consent) sharing of records with researchers under some conditions and disclosure is permissible with parental consent.

What protection do student records have in the hands of external researchers? Unfortunately, the answer is generally none. FERPA does not apply to researchers. The law only applies to schools. FERPA protections do not follow records when disclosed to researchers. Therefore, in the hands of researchers, student records only have the privacy and security protections that the researchers themselves provide.

Academic researchers must obtain approval for their activities from an institutional review board (IRB), as required by human subjects protection regulations of the federal government. These regulations are known as the Common Rule because many federal agencies subscribe to the same set of research rules. IRBs can and should impose privacy and security requirements because it is their role to look out for the interests of data subjects. IRBs should ensure that researchers take all necessary steps to protect the privacy and other interests of data subjects, especially children.

I recently had the opportunity to review a university research project involving students that is foundation funded. The research subjects of the project being conducted by faculty at the State University of New York at New Paltz are grade-schoolers whose parents agreed to let them participate. A goal of the project apparently was to determine if providing one-on-one instruction to

students would help them learn. (There already is abundant research showing that tutoring helps students learn more effectively, so arguably this project is not critical to our understanding of teaching and learning.)

The original research proposal did not address any privacy and security issues in regard to student data. The words privacy, security, and confidentiality did not appear in the draft that I saw.

The researchers also wanted access to records of students who did not participate in the project because they served as the controls to show whether the extra attention the student participant received made a difference. While the researchers obtained the consent of a parent for student participants, they did not intend to provide notice or seek consent from students whose records were the controls. This is disturbing. When there is neither notice to, nor consent received from, parents of students in the control group, there is ample opportunity for violations of privacy and security. The researchers also did not address the privacy interests of student teachers who provide the tutoring.

My questions to the researchers about privacy and security for the students involved did yield some measures on their part to institute protections. But they were not enough. I followed up with the SUNY New Paltz IRB to learn if the Board would require more of the researchers. I wrote to the IRB detailing specific objections to the privacy and security measures for the research study. My hope was that the IRB would ask the researchers to do more, but the Board's response was terse and dismissive of privacy concerns. In a one-paragraph letter, the IRB stated that it reviewed my concerns and that it believed the researchers will use adequate privacy and security safeguards. In other words, trust us and go away.

The IRB offered no actual evidence that it cared about privacy and security. The students in the project deserved better than this. I sent a second letter to the IRB and also made a request under the New York State Freedom of Information Law (FOIL) for records of the IRB's deliberations. I did receive a response to my FOIL request with some of the items I requested, including the minutes of a meeting during which my first letter was discussed. The minutes showed that my original letter resulted in a few sentences of mention, but that portion of the minutes was withheld. Most of the material from a later IRB meeting with the researchers also were withheld. Why the IRB insisted on avoiding public scrutiny of its activities is unclear. The IRB could have disclosed its deliberations and showed that it did its due diligence. Its refusal to be transparent suggests that it may have something to hide.

I will not pursue here the University's violations of the FOIL's standards and procedures, but IRB minutes that were disclosed indicate that the researchers told the IRB that "students will not be identifiable and all data will be confidential." The first part of that statement is patently untrue. The students being tutored are obviously identifiable. The researchers, tutors, and maybe others will have records about identifiable students. Perhaps at some point all identifiers will be removed, but it takes a lot of effort to make records truly non-identifiable. You cannot simply remove names to make the records non-identifiable, because it is often easy to re-identify records. In any event, the researchers must keep consent forms from parents for a period of time in case of litigation or oversight. Did the IRB require the researcher to detail how they

planned to de-identify the records? Not in any way that was evident. Could the IRB know whether a de-identification method is sufficient? That also cannot be verified.

The researcher's statement that "all data will be confidential" is largely meaningless by itself and would not be acceptable to anyone with knowledge and expertise in data and personal privacy. In order to assess confidentiality, it is necessary to know the policy controlling use and disclosure. Will the "confidential" records be disclosed in response to a subpoena? Will the "confidential" records be disclosed to the IRB or to research fraud investigators? Will the "confidential" records be stored in the cloud or shared via insecure email? As far as the SUNY New Paltz IRB is concerned, the statement by researchers that data will be "confidential" is sufficient. Whether the IRB members understand the implication of their policy is unclear.

In my FOIL request, I also requested a copy of the standards used by the IRB to evaluate research proposals. After all, if you are tasked with assessing privacy and security protections, you must have standards to measure the protections against. The response is telling. The University said only that the IRB "follows federal regulations for the protection of human subjects known as the "Common Rule."

However, there are not any security and privacy standards in the Common Rule. The Common Rule is a broad and vague requirement for "adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data." The Rule requires additional but unspecified safeguards for vulnerable populations, including children. Does the Common Rule require the use of passwords to protect data? Encryption? Does a research project need a privacy policy that meets recognized standards like Fair Information Practices? All these very important questions are not addressed by the Common Rule.

So, SUNY New Paltz points to the Common Rule, which only points back to the IRB. But the evidence suggests that the SUNY New Paltz IRB does not have any privacy or security standards at all. While this is one example of how a university IRB deals with privacy and security concerns, the questions raised should be asked of any researcher studying students and student data.

IRBs are the first line of defense for the protection of student research subjects. If they do not do their job, then parents, educators, and government officials must ask tough questions of these boards and ensure that they are held to the highest standards of protecting students' privacy and security.