Privacy HOLEs in the ‘Hidden Healthcare System’

STUDENTS’ PHI-LADEN EDUCATION RECORDS THAT ARE STORED AND SHARED ELECTRONICALLY DON’T HAVE THE SAME SAFEGUARDS AS MOST EHRS

By Daniel A. DuBravec, CHTS, CEHRS, and Matt Daigle
WITH STUDENT SAFETY and privacy an increasing parental concern, school administrators nationwide are sitting on a powder keg of potential backlash because of a gray area of student privacy protections that Julia Lear, senior advisor for the Center of Health and Health Care in Schools at George Washington University, calls the “hidden healthcare system.”

Lear’s “hidden healthcare system” exists in every town, every county, and every state. It’s a mottled system, attending to the needs of nearly 50 million students in approximately 100,000 public schools. Another 40,480 private and religious K–12 schools require health services. Within the schools themselves, the healthcare system is varied, with some having a large staff of full-time school nurses while others share a single nurse amongst multiple schools and can rely on unlicensed assistive personnel as needed.

Equally varied is how school districts document care and treatment. When a student is treated by a school nurse, the medical encounter is often entered into a system using the district’s software of choice. Sometimes this software is maintained by the school on the local network; other times it is hosted by a vendor as a cloud-based application. A vast majority of survey respondents (59 percent) told the National Association of School Nurses that they use electronic health records (EHRs) to document student health data containing treatment notes, screenings, and sometimes medical charts.

The privacy and security of this medical information can vary, and some are concerned that not enough is being done to protect this hidden healthcare system’s medical records.

Students Left Behind
At a federal level, health record privacy concerns have given rise to a number of laws and regulations. The best known of these is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA was enacted in 1996 to establish transaction, security, privacy, and other safeguards to protect health information when stored and shared electronically. It is specifically created for healthcare providers (or “covered entities”) who conduct electronic transactions that contain patient information. K–12 schools would only be considered “covered entities” if they were electronically billing Medicaid-covered services from the school location. Since medical data recorded by the schools is stored and classified as an education record, it does not fall under HIPAA. Instead, education records are covered by a different federal law, the Family Educational Rights and Privacy Act (FERPA).

FERPA was created specifically for the privacy of student records as a whole, allowing parents the right to access and review student records, make modifications if they are incorrect, and to grant disclosure of the records. This law ensures student record confidentiality to the extent that it sets some limitations for how the information is shared. In fact, FERPA only provides protections to schools that receive federal funds. Therefore, students of private and religious schools often find themselves without any federal protection by either HIPAA or FERPA.

Parents in many cases carry a common, false assumption that this medical data captured by nurses at local schools and local clinics are equally protected by HIPAA, and, if not, FERPA.

HIPAA security rules, and the security risk assessment tools based thereon (such as those recently released by the US Department of Health and Human Services (HHS)) were designed to protect patient data, but the same focus on electronic protected health information (e-PHI) does not appear to extend to students attending K–12 schools.

In the US, schools compile detailed and robust “education records” directly related to each student, and these records are maintained by an educational agency, institution, or party acting on behalf of the institution. There are many components of this record, including: the cumulative file; the clinic file; the disciplinary file; the special services file; and the English for Speakers of Other Languages (ESOL) file.

For students attending a K–12 school, health information recorded by a school nurse is not classified as a medical record, but rather is combined with all the students’ education and demographic information. The clinic file can also contain many medical record file types, such as annual health data, cumulative health records, emergency care information, general health information, and medical flag information. Here’s where things start to become gray—when this type of data is collected by K–12 schools electronically, the only distinction between it and the data stored at a clinic or hospital in an EHR are the laws which govern it and any established legal safeguards.

Where are the Safeguards?
A review of current guidelines and laws found that there are many concerning areas related to electronic student medical information security within K–12 schools. It raises a critical question: Do public, private, and parochial K–12 schools have administrative, physical, and technical safeguards in place for their electronic data—which includes medical and other privacy information—when it is being shared with K–12 administrative staff, faculty, school volunteers, and sometimes even software vendors?

The authors found that there are a number of developing trends that should be worrisome to school administrators:
• In general, the majority of K–12 schools do not fall under HIPAA protection and guidance. If those same records were stored by local clinics or hospitals, federal mandates would call for HIPAA protection and the issuance of fines if those laws were violated.
• Public K–12 schools do fall under FERPA federal privacy regulations, but not for medical records, and private institutions have even fewer protections. Similar HIPAA-like privacy guidelines for administrative, physical, and technical safeguards are minimal to non-existent. Private or religious schools are not subject to HIPAA or FERPA guidelines.
• Data is at risk whether from negligent behavior or from malicious attacks. New reports and studies indicate a growing awareness and concern that sensitive student data is poorly protected and improperly shared, or being intentionally hacked due to weak security safeguards. For example, in early 2014, Loudoun County Public Schools discovered that personal information about students and staff members was publicly available—not because of the efforts of a clever or disgruntled hacker, but rather by a third-party vendor contracted by Loudoun County who failed to implement password protections within their software. This allowed more than 1,300 links to the school’s confidential in-
formation to be accessible by any Internet user with access to Google. This is an example of only one school system out of thousands who find themselves in similar situations.

- **FERPA does not contain specific breach notification requirements when sensitive data is hacked or released through employee negligence.** A breach of this type does require the school to record the incident, but it’s the school’s prerogative whether to notify parents or guardians about a breach.

### Student Health Data Faces Many Risks

A recent survey revealed that more than 40 percent of schools use cloud applications to store their data. If you read the privacy policy of these vendors, you’ll notice that nearly all have a clause that some of the data might be shared and their privacy policy may change at any time. A 2013 report by Fordham University’s Center on Law and Information Privacy revealed none of the schools surveyed by the authors had a contract in place requiring the hosting cloud service provider to notify the school if the service provider becomes a target of a data breach.

There are other concerns with “the cloud.” The recent bankruptcy of software vendor ConnectEDU forced the intervention of the Federal Trade Commission to prevent 20 million student records from being sold to a venture capital company. Another complication is where the cloud emanates from—especially when the servers that hold the data aren’t located in the United States. Very few K-12 schools are aware of the student data privacy risks presented by foreign storage of US student data.

The varied nature of school personnel also presents its own challenges. Student medical data may be viewed by more than just the school nurse or the current classroom instructor due to lax school policies or limited access control from poorly designed software. This opens the door to legal access by anyone who may be on the school’s staff under the auspices of legitimate educational interest, which can include parents and community volunteers, since it is highly unlikely that the school administration requires volunteers to sign non-disclosure agreements to prevent them from revealing what they might see in a student’s record.

That’s not to discourage the use or downplay the benefits of storing student data electronically in K-12 school systems, especially in a fiscally challenging environment. School budget savings can be expected to reach 27 percent by 2016 by shifting paper-based or local network applications to cloud computing servers.

Also, the resulting increase in the usefulness of these records has allowed K-12 school systems to more effectively use student EHRs to track immunizations, concussions, and the prevalence of flu viruses. Just like with traditional hospital EHRs, student electronic records also allow school nurses to more effectively track medication doses they have administered. These rewards further reinforce the urgency of the matter—that immediate attention and local, state, and federal legislation needs to be the priority of school administrators.

If action isn’t taken soon, school systems will ultimately be mired in litigation as student data is exposed in large scale breaches because proper security protections were ignored or deemed too costly to implement. One solution would be the broader application of HHS’ HIPAA guidelines, which can be used just as effectively within the K-12 school environment. Also, since student records contain medical information, relevant software should be required to go through an EHR certification process similar to what the Office of the National Coordinator for Health IT requires of EHRs that are to be used by hospitals and clinics.

### More Legislation Needed to Protect Data

The strange dichotomy of how student medical data is treated differently by K-12 schools versus medical data stored by EHRs in hospitals has not gone unnoticed. In 2012, the Electronic Privacy Information Center (EPIC) brought legal action against the US Department of Education to challenge FERPA’s current guidelines. Unfortunately, the court dismissed the lawsuit stating that EPIC did not have standing to bring the claims asserted in the complaint. The issue seems to be reaching a crossroads in 2015. An April 17, 2015 *Washington Post* article on Virginia’s legislative efforts to ensure parents are notified of school data breaches states that “in the first three months of 2015 more than 160 bills were introduced in 41 state legislatures to address education data privacy.” Of these states, California implemented the Student Online Personal Information Protection Act, which since January 1, 2015 prohibits operators of Internet websites or online services from disclosing, compiling, or selling student data.

At a federal level, President Barack Obama urged Congress to impose similar restrictions. Google, Apple, Microsoft, and 73 education technology providers have pledged to follow the Future of Privacy Forum (FPF) and the Software and Information Industry Association (SIIA) Student Privacy Pledge to protect students from the collection, maintenance, and use of student personal information by software vendors.

In reality, these efforts only go so far. Granted, they will offer some cursory protections against the sharing of student data with external vendors. But how this data is shared internally within the individual schools and school systems remains a massive concern. Only by requiring mandatory national guidelines of administrative, physical, and technical safeguards specified by HIPAA will student data then have the same privacy protections as all other electronic medical records.

### Notes


Daniel A. DuBravec (ddubravec@lmi.org) is a senior consultant at LMI, a nonprofit government consulting firm. DuBravec holds multiple EHR certifications and is a consultant for the government on EHR patient privacy and security standards. Matt Daigle (mdaigle@lmi.org) is senior public affairs specialist for LMI and holds a master’s degree in journalism from Northwestern University.