

Chair Doherty and members of the House Education Committee,

Please pass HB 2712. This bill directs the State Board of Education to adopt a schedule of civil penalties for violations of rules related to creation, use, custody and disclosure, including access, of student education records.

This bill should also specifically address the records held by third party vendors on behalf of SEAs and LEAs.

A physician, I advocate for stronger data privacy protections in both education and healthcare. ARRA stimulus was used to incentivize digitalization of health care[1] and education.[2]

HIPAA rule changes eliminated the “right of consent,”[3] replacing the privacy rule with regulatory permission to disclose protected health information.

1996	Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HSS) was required to develop regulations that specified patients' rights to health privacy.	<i>"...the Secretary of Health and Human Services shall submit to [Congress]... detailed recommendations on standards with respect to the privacy of individually identifiable health information."</i>
2001	President Bush implemented the HHS HIPAA "Privacy Rule" which recognized the "right of consent".	<i>"...a covered healthcare provider must obtain the individual's consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment or health care operations."</i>
2002	HHS amended the HIPAA "Privacy Rule", eliminating the "right of consent".	<i>"The consent provisions... are replaced with a new provision...that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, or health care operations."</i>

In six years, I predict we'll see Anthem-size data breaches in education unless holes in FERPA are corrected. HIPAA had a head start on FERPA.

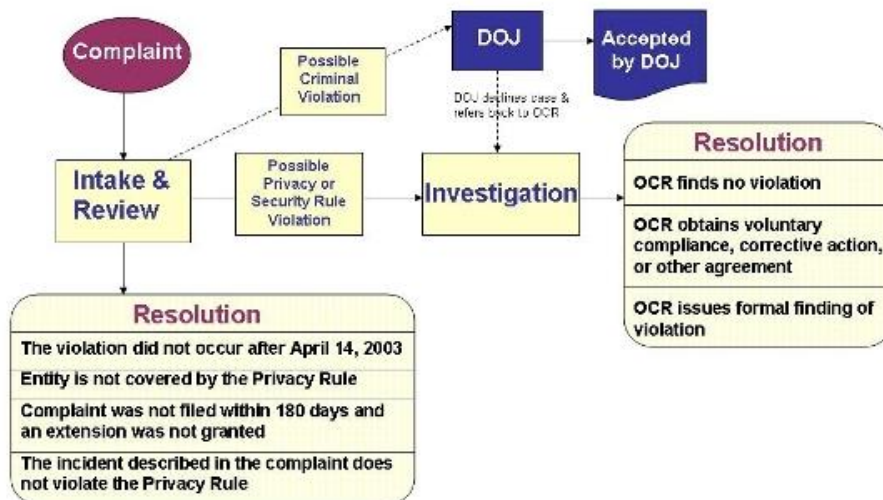
Before 2008, FERPA accommodated research projects seeking nonconsensual access to personally identifiable information (PII) to improve instruction, administer student aid, or to develop, validate, or administer predictive tests. Subsequently (in 2008 and 2011) FERPA rules were changed to expand non-consensual disclosure of PII from education records.[4]

In *Doe v. Gonzaga University*[5], the Supreme Court ruled that FERPA does not grant any personal rights to enforce under the civil rights provisions of Section 1983, since the statute only allows for withholding of federal funding for violations—and this stick is deemed too draconian to ever use

The Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification Rule requires HIPAA-covered entities to notify HHS of a breach of unsecured protected health information. Breaches of unsecured protected health information affecting 500 or more individuals posted.[\[6\]](#)

HIPAA, like FERPA, has no private right of action. However, HIPAA Privacy and Security violations could ensue in fines[\[7\]](#).

### HIPAA Privacy & Security Rule Complaint Process



- In July 2013, Wellpoint paid HHS \$1.7 M for a breach security weaknesses in an online application database that left electronic protected health information (ePHI) of 612,402 individuals accessible to unauthorized individuals over the Internet.[\[8\]](#)
- State agencies[\[9\]](#) and county governments[\[10\]](#) have paid fines for potential HIPAA violations.
- A New York and Presbyterian Hospital (\$3.3 M) and Columbia Hospital (\$1.5 M) agreed to record high fines of \$4.8 M.[\[11\]](#)
- Beginning Sept. 23, 2013, liability for many of HIPAA’s requirements will extend directly to business associates that receive or store protected health information, such as contractors and subcontractors.

In the first HIPAA audit[\[12\]](#) completed by HHS OCR last year, 58 of 59 covered had at least one negative finding. In 2015, HHS OCR will shift their focus to auditing business associates. Compliance “sticks” have not been in place sufficiently long enough to know how effective they will be.

But any time new technology is introduced, new wrinkles appear. Telemedicine is an example that may impact LEAs serving the student community with school-based healthcare. The HIPAA security rule does not apply to video conferencing because “the information being exchanged did not exist in electronic form prior to the transmission.” If, however, there is a breach of personal health information, practitioners and the LEA could be on the hook. I hope you read my commentary in the current issue of the Lund Report.[\[13\]](#)

The idea that the HIPAA security rule doesn't apply to videoconferencing may be true of students' use of a digital medium for browsing, assessments and other real-time activities. Those activities are not education records. The Supreme Court ruling of *Owasso Independent School District v. Falvo*[\[14\]](#) held in favor of the school district in deciding that students scoring each other's tests and calling out the grades does not violate FERPA. FERPA defines education records as "records, files, documents and other materials" containing information directly related to a student, "maintained by an educational agency or institution or by a person acting for such an agency or institution."[\[15\]](#)

HB 2712 is an important bill that addresses FERPA enforcement. Please support this bill.

Kris Alman M.D.

---

[\[1\]http://www.cisco.com/web/strategy/docs/healthcare/09CS2146\\_FAQ\\_ARRA\\_HIT\\_Stim\\_r1\\_052709.pdf](http://www.cisco.com/web/strategy/docs/healthcare/09CS2146_FAQ_ARRA_HIT_Stim_r1_052709.pdf)

[\[2\] http://nces.ed.gov/programs/SLDS/fy09arra\\_announcement.asp](http://nces.ed.gov/programs/SLDS/fy09arra_announcement.asp)

[\[3\] http://patientprivacyrights.org/truth-hipaa/](http://patientprivacyrights.org/truth-hipaa/)

[\[4\] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html](http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html)  
<https://epic.org/foia/ed/ferpa/default.html>

[http://ptac.ed.gov/sites/default/files/webinar-data-sharing-011112\\_final.pdf](http://ptac.ed.gov/sites/default/files/webinar-data-sharing-011112_final.pdf)

[\[5\] http://ferpaguide.org/?page\\_id=51](http://ferpaguide.org/?page_id=51)

[\[6\] As required by section 13402\(e\)\(4\) of the HITECH Act  
https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

[\[7\] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html)

[\[8\] http://www.hhs.gov/news/press/2013pres/07/20130711b.html](http://www.hhs.gov/news/press/2013pres/07/20130711b.html)

[\[9\] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs)

[10] <http://www.hhs.gov/news/press/2014pres/03/20140307a.html>

[11] <http://www.hhs.gov/news/press/2014pres/05/20140507b.html>

[12] [http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference\\_Handouts/Compliance\\_Institute/2014/tue/710print2.pdf](http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf)

[13] <https://www.thelundreport.org/content/opinion-privacy-risks-climb-era-big-data>

[14] <http://www.law.cornell.edu/supct/html/00-1073.ZO.html>

[15] <http://www.rcfp.org/browse-media-law-resources/news/high-court-finds-education-records-law-not-violated-peer-grading>