Chair Doherty and members of the House Education Committee,

I support HB 2710. This bill would require the State Department of Education to issue a privacy risk assessment of any data system, program or contract involving student education records.

Until last month, Becky Straus directed ACLU's advocacy and lobbying efforts. In one of her last responsibilities for ACLU, she gave a talk to a combined audience for the World Affairs Council and Portland State University. When asked how she keeps up with all the privacy issues in Oregon, she admitted she couldn't. She said that Oregon should have a Chief Privacy Officer.

Yesterday, the House Subcommittee on Early Childhood, Elementary, and Secondary Education[1] held hearings on **"How Emerging Technology Affects Student Privacy."** Congresswoman Bonamici, CD-1 made these opening comments. "I hear a lot from my constituents in Oregon who are as concerned as I am about the gaps in protection." She noted, "Technology changes much fast than policy changes."

Mr. Joel Reidenberg[2] testified before this committee—as he done multiple times before Congress. His final recommendation in a Center on Law and Information Policy report in 2008[3] stated:

> *States should have a **Chief Privacy Officer** in the department of education who assures that privacy protections are implemented for any educational record database and who publicly reports **privacy impact assessments** for database programs, proposals, and vendor contracts*.

This recommendation is notable because Reidenberg gave Congress the same advice today. States need CPOs.

In 2013, Senator Mark Hass held a hearing on behalf of Oregon Save Our Schools to address student privacy. SB 567[4] would have created a Chief Privacy Officer. But I said then, as I do now, that Oregon should follow Ohio's lead. Ohio's CPO and Chief Information Security Officer oversee the Privacy and Security Information Center[5] which "acts as a privacy and security knowledge center for the citizens, businesses, and employees of the State of Ohio."

The CPO and CIO, with input from State and Local Education Agencies, teachers, parents and students, could give guidance for proposed legislation and enforcement of the three federal privacy statutes that address student information that may be collected by and from schools: the Family Educational Rights and Privacy Act of 1974 ("FERPA")[6], the Children's Online Privacy Protection Act ("COPPA")[7], and the Protection of Pupil Rights Amendment ("PPRA")[8].

The demand for Big Data means more and more data will be collected, shared and sold between agencies, nonprofits and third party vendors and potentially spanning an individual's lifetime. This means that other laws and agencies that protect privacy must be considered. HIPAA collides with FERPA when a student has a chronic medical condition, like diabetes.

As a retired endocrinologist, I am very concerned about how school-based health centers[9] will be handling health data. Telemedicine could be useful for SBHC as the lobbyist for the Telehealth Alliance of Oregon notes in her testimony supporting SB 144.[10] But telemedicine law is inadequate. The HIPAA security rule does not protect teleconferencing.[11]

I hope you read my critique of this bill, which is in the current edition of the Lund Report.[12]

Please support this bill and consider creation of an Oregon Chief Privacy Officer and Privacy and Security Information Center.

Kris Alman, MD

---

[1] Her testimony begins at 1:19:45 https://www.youtube.com/watch?v=zWgfszB03V0
[2] Stanley D. and Nikki Waxberg Chair and Professor of Law; Founding Academic Director, Center on Law and Information Policy http://law.fordham.edu/faculty/joelreidenberg.htm

[3] https://epic.org/apa/ferpa/Fordham%20Center%20Report.pdf CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS

[4] https://olis.leg.state.or.us/liz/2013R1/Downloads/MeasureDocument/SB567

[5] http://www.privacy.ohio.gov/

[6] http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[7] http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[8] http://www2.ed.gov/policy/gen/guid/fpco/ppra/index.html

[9] http://osbha.org/sbhc/why

[10] https://olis.leg.state.or.us/liz/2015R1/Downloads/CommitteeMeetingDocument/43353

[11] "As defined in the Security Rule, ePHI (Protected Health Information)… does not include paper-to-paper faxes, video teleconferencing, or messages left on voice mail—because the information being exchanged did not exist in electronic form prior to the transmission." http://bit.ly/1AgKqoK

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