

Chair Fagan and members of the House Committee on Consumer Protection and Government Effectiveness:

[HB 3099](#) would create a State Chief Information Officer whose primary role is to advise the governor regarding information technology and telecommunication.

This bill should be amended to create a [Privacy and Security Information Center](#) and the position of both a State Chief Information Officer and a Chief Privacy Officer similar to what Ohio has done.

The reason? Consider the mess with FERPA & HIPAA in regards to the U. of O. debacle. (See my testimony for today's House Judiciary hearing on [HB 3476](#).)

A sampling of backgrounds for your committee members includes a former David Douglas School Board member (Rep. Fagan), a physician (Dr. Buehler), a former computer support technician (Rep. Nearman), a civil rights lawyer (Rep. Rayfield) and a former teacher (Rep. McClain).

But it doesn't take this wealth of experience to realize that technology is outpacing the laws that protect citizens in the era of big data.

Case point: The University of Oregon's bungling with HIPAA and FERPA.

Please create an Oregon State Privacy and Security Information Center with both a CIO and CPO at the helm. This center should guide the governor and the legislature; and it should be a resource for citizens to protect their confidential data and to report cybercrime.

My husband and I sure could have used a center like this after we experience identity theft when filing our federal taxes last year!

Kris Alman

----- Forwarded message -----

From: **kris alman** <kris.alman@gmail.com>

Date: Tue, Mar 24, 2015 at 2:02 PM

Subject: Testimony for public record HB 3476: privacy, HIPAA and FERPA

To: rep.jeffbarker@state.or.us, rep.brentbarton@state.or.us, Rep.MitchGreenlick@state.or.us, rep.waynekrieger@state.or.us, Rep.AnnLininger@state.or.us, Rep.BillPost@state.or.us, REP Sprenger <rep.sherriesprenger@state.or.us>, Rep Williamson <Rep.JenniferWilliamson@state.or.us>, Rep.AndyOlson@state.or.us

Cc: channa.newell@state.or.us, eric.deitrick@state.or.us, laura.handzel@state.or.us, jeff.rhoades@state.or.us, mike.reiley@state.or.us, kristi.arrington@state.or.us, danguole.lekaviciute@state.or.us, Senator Gelser <Sen.SaraGelser@state.or.us>, sen.jackiewinters@state.or.us, Sen Prozanski <sen.floydprozanski@state.or.us>

Rep.VicGilliam@state.or.us, REP Huffman <Rep.JohnHuffman@state.or.us>, REP Johnson <rep.markjohnson@state.or.us>, Rep Piluso <Rep.CarlaPiluso@state.or.us>, Rep Read <rep.tobiasread@state.or.us>, Rep.KathleenTaylor@state.or.us, Rep VegaPederson <Rep.JessicaVegaPederson@state.or.us>, sen.brianboquist@state.or.us, SEN Devlin <sen.richarddevlin@state.or.us>, Sen.BillHansell@state.or.us, Sen Kruse <sen.jeffkruse@state.or.us>, Arnie Roblan <Sen.ArnieRoblan@state.or.us>, Kimberly McCullough <kmccullough@aclu-or.org>, "Rep. Lew Frederick" <rep.lewfrederick@state.or.us>, Kushner Jonah L <jonah.l.kushner@state.or.us>

Chair Barker, members of the House Judiciary Committee and sponsors/co-sponsors of HB 3476,

HB 3476, while commendable, would deny a college's legal defense team access to mental health records of domestic violence, sexual assault and stalking victims. In a bipartisan way, Oregon legislators are clearly concerned about the behaviors of U. of O. administrators. This is not surprising since privacy is a bipartisan issue.

However, the problem at U. of O. is rooted in FERPA and HIPAA. FERPA's original intent is undermined when education records include health records. This will extend beyond colleges to k-12 schools delivering care at school-based health centers. Telemedicine poses additional hazards.

Students should not be second-class citizens when they receive their health care through schools.

FERPA and HIPAA rule changes accommodate a digital economy when loosened rules promote disclosures of confidential information without consent. This puts all students at great risk.

While Congress is beginning to respond to parents concerned about student data privacy, there is surprisingly little being done to address health data privacy--despite massive data breaches this year. **The Oregon legislature should pass a resolution asking Congress to address the failures of FERPA and HIPAA in protecting confidential data.**

- Oregon House [Bill 3476](#) should:
 - o Limit health data in education records to vaccines; and

o Require all public schools to become a “[hybrid entity](#),” designating the health unit (including the school-based health center) as a “health care component”. This separate legal entity would follow HIPAA privacy and security rules.

- The Oregon legislature should create a [Privacy and Security Information Center](#) and hire a Chief Privacy Officer similar to what Ohio has done
- The Oregon legislature should pass bills championed by Rep. Lew Frederick that protect student privacy: [HB 2708](#), [HB 2709](#), [HB 2710](#), [HB 2711](#), and [HB 2712](#); and bills that assure better communication with family members and outpatient management for all individuals suffering with mental illness: [HB 2022](#), [HB 2023](#) and [HB 2948](#)
- The House should not pass [SB 144A](#) without amendments that stipulate telemedicine shall comply with the HIPAA Security Rule and that guidelines for encryption are established.

I hope to give oral testimony tomorrow, but I want to also do so for Senate Health Committee hearings on price transparency at the exact same time.

- [SB 891](#) Requires health care facilities to publish, in manner prescribed by Oregon Health Authority, price data regarding health care services offered.
- [SB 900](#) Requires Oregon Health Authority to be responsible for posting to its website health care price data for inpatient and outpatient hospital services.
- [SB 665](#) Creates Hospital Rate Commission in Oregon Health Authority to review hospital charges billed by certain hospitals and recommend to Oregon Health Authority whether to approve charges as reasonable based on prescribed criteria.

In many ways it's the same story. Our confidential health data is sent without consent to Milliman Inc., a global actuarial firm, that is the vendor for Oregon's two All Payer All Claims databases. Patients cannot access allowed and negotiated prices for plans when buying their premiums or seeking care in the community. That's because health plans and hospitals claim negotiated prices are a "trade secret." Who knows if Milliman is re-purposing the data? [Milliman has already been in trouble with the FTC](#) so it wouldn't be surprising...

Discussion is below.

Thank you,

Kris Alman MD

If Duck fans were disappointed with the National Bowl Championships, they should roundly boo the university's handling of a Title IX lawsuit. Katie Rose Guest Pryal (a former University of North Carolina professor of law who specializes in higher education, mental health, and social-justice issues) struck a nerve in the Chronicle of Higher Education when she recently wrote this commentary: ["Raped on Campus? Don't Trust Your College to Do the Right Thing"](#)

Earlier this year, the [University of Virginia](#) was the epicenter of controversy for college rape cases. Alcohol and sex flow with abandon in colleges where a [hookup culture](#) is prevalent. The Rolling Stones took a hit for their investigations when a police report of ["discrepancies"](#) resulted in a magazine apology.

Now the spotlight is on University of Oregon, where a negative shadow is cast on [administrators who obtained a student's counseling records without her consent](#). This happened after she sued the university and the men's basketball coach Dana Altman in a [Title IX complaint](#). The lawsuit claims coaches were fully aware a highly prized recruit, Brandon Austin, was suspended from Providence College following an allegation of gang rape in November 2013 when they recruited him. Austin's mother stated, "We told them everything. They knew everything."

Merely four months later, an 18 year-old U. of O. student alleged Austin and two other basketball players gang-raped her.

The U. of O. intended to use the student's own post-rape therapy records against her. Never mind that the student wasn't suing the [University Counseling & Testing Center](#) for her care there. (That would be an [exception to psychotherapist-patient privilege protections](#).)

So egregious are the U. of O's actions, they now merit two of the six footnotes of the [current Wikipedia entry on FERPA](#). Google "nonconsensual" and you see this sample sentence.

nonconsensual - definition of **nonconsensual** by The Free ...

The results are a first glimpse into how many UO students may be victims of sexual assault or **nonconsensual** sexual experience during their time on campus.

 thefreedictionary.com/nonconsensual

[HIPAA rule changes in 2002](#) and FERPA rule changes in [2008](#) and [2011](#) remove consent and allow nonconsensual disclosure of medical and health records.

The U. of O. debacle must therefore prompt deeper discussions and national solutions to assure that both students' health records *and* privilege laws are protected. [Senator Wyden](#)

and Congress, rather than U.S. Secretary of Education Arne Duncan, should clarify “clarify how FERPA applies to student medical records.”

FERPA applies to educational agencies and institutions that receive funds under any program administered by the U.S. Department of Education. Technically, FERPA (the Family Education Rights and Privacy Act) is on the side of U. of O.

[Under what conditions is prior consent not required to disclose information?](#) *If a parent or eligible student initiates legal action against an educational agency or institution, the educational agency or institution may disclose to the court, without a court order or subpoena, the student's education records that are relevant for the educational agency or institution to defend itself.*

Moreover, most colleges operate student health centers. As such, students’ health records (for the most part) are deemed “education records,” and [FERPA privacy rules apply](#).

Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to establish national standards and requirements for electronic health care transactions and to protect the privacy and security of individually identifiable health information. The HIPAA privacy rule simply does not apply to most students’ health records because the [US Department of Health and Human Services has ruled](#) that *"individually identifiable health information that is part of an 'education record'... would not be considered protected health information."*

In 2010, former U.S. Senator James Buckley called for Congress to amend FERPA because college athletic departments were using the statute to hide payoffs made to students in violation of NCAA regulations and sexual abuse committed by student athletes. Buckley wrote FERPA in 1974 to help parents access their children’s educational records. [He said](#), “One problem is this law was passed over 40 years ago, and all kinds of interpretations were added over time. I do know college administrations have played a lot of games with it.”

Ethicists examining the U. of O. case were quick to notice counselor [Jennifer Morlok’s letter of concern](#) citing her duty to report prohibited or unprofessional conduct. She pointed out that, “(I)t is our job to protect our client’s clinical information.”

Morlok draws our attention to the FERPA loophole that conflicts with patient privilege laws. *All states* recognize the [psychotherapist-patient privilege](#), and the privilege is also recognized under federal common law. Unfortunately, this only applies to federal court proceedings.

In Oregon, a [psychotherapist](#) means a person who is:

(A) Licensed, registered, certified or otherwise authorized under the laws of any state to engage in the diagnosis or treatment of a mental or emotional condition; or

(B) Reasonably believed by the patient so to be, while so engaged.

The [U.S. Federal Rules of Evidence](#) do not recognize [doctor-patient privilege](#), but most states, including [Oregon](#), do. What about counselors, psychologist, social workers or nurses working in schools? Wouldn't parents and students reasonably believe mental and emotional conditions are privileged discussions in schools? Indeed, Oregon also recognizes the [school employee-student privilege](#).

Mental health records are afforded more protections. A [Supreme Court ruling](#) clarifies this. "Effective psychotherapy... depends upon an atmosphere of confidence and trust in which the patient is willing to make a frank and complete disclosure of facts, emotions, memories, and fears... (T)he mere possibility of disclosure may impede disclosure of the confidential relationship necessary for successful treatment." Unfortunately, this ruling applies to only federal court proceedings.

The [HIPAA privacy rule](#), not FERPA, permits a health care worker to share an incapacitated patient's information with family, friends, or others if it is in the best interests of the patient.

Confidential data is at the heart of the U. of O controversy. Confidential data that is both mined and heavily guarded by institutions to their benefit. Confidential data that is shared without notice and consent and without appropriate safeguards to assure privacy and safety for students. Students should have [a right to privacy for both health care and education](#).

The last time there was [joint guidance on HIPAA and FERPA](#) was in 2008. This guidance is woefully out-of-date since FERPA rules and regulations were subsequently relaxed to collect and share more data. They've become a bigger headache in the digital era because seemingly infinite bytes of data can be collected and shared without notice and consent. Surveillance, commercial exploitation, profiling and cybercrime are intended and unintended consequences.

Both finance *and* research prompt bigger and bigger data in the digital era. HIPAA's privacy and security rules enable money and data to flow through a complicated web of ["covered entities."](#) We see how well that has been working since two major data breaches affecting patients were reported this year: [80 million Anthem Blue Cross patients](#) are at risk for **identity theft**; and, more recently, [11 million Premera BlueCross](#) patients are also at risk for **medical identity theft** since both medical data and financial information was breached.

But [parents aren't happy with FERPA](#) either. They're concerned that companies could share sensitive details like students' grades, disciplinary actions or health data. In Arizona, [a family's](#)

[medically fragile 4-year old son received two unauthorized and unnecessary "baby root canals"](#) while being forcibly held down inside his school after ReachOut Healthcare America (a corporate dental chain) inappropriately accessed his student records. Parents are also worried that college or job recruiters could get access to records that adversely profile their kids.

Parents are also worried about data breaches and identity theft. That's not unreasonable since [thirty educational institutions experienced data breaches](#) last year—among them, the [medical and financial data of UC Irvine Student Health Center patients](#).

Big data spurs research in the guise of accountability. [Columbia University's Current Issues in Research Ethics](#) sums up their concerns: "Given our modern research setting, with its growing dependence on computers, the Internet, and with the need for databases and registries, protection of an individual's privacy is now one of the greatest challenges in research."

The Office for Civil Rights in Health and Human Services monitors health care data breaches. Acknowledging how rarely fines are imposed, the director, [Jocelyn Samuels, still asserts](#) patients can "entrust their providers with this really intimate information knowing that it won't be misused or inappropriately disclosed" despite new threats and smarter cybercriminals.

New healthcare delivery models in schools and technology pose new threats.

- **School-based health centers (SBHC) serving k-12 students**
- **Student Information Systems**
- **Telemedicine**

These threats result from privacy and security laws that are inadequate, inconsistent, and incomprehensible and from "education records" that go far beyond test scores.

The [Oregon School Nurses Association](#) advocates for "a form and structure to collect 'hard data,' creating a bridge between the world of health and education, and look at ways to fund school nursing services outside of the Department of Education's budget." One way to do that would be to [bill students' health insurance](#). If the Gordian knot of funding school nursing services is "solved" through billing insurance, the question of record keeping becomes a new Gordian knot.

[The Public Health Division](#) of the Oregon Health Authority writes the rules for school-based health centers. [Certification of SBHCs](#) in Oregon is voluntary. While standards for certification include confidential phone messages and faxes, there are no explicit standards for how data is stored and transmitted—only that SBHCs must have an information sharing policy between school nurse and SBHC staff.

All certified SBHCs must collect data, including a unique patient identifier, date of birth, gender, site identification, CPT and diagnostic codes. **This data set is clearly [not de-identified information](#) according to the HIPAA privacy rule "safe harbor" method.**

Current Issues in Research Ethics identifies children, the cognitively impaired, and substance abusers among [vulnerable populations](#) for which researchers must be sensitive. They caution the use of “safe harbor” and “statistically de-identified” data sets. Re-identification is possible when data mining tools are used with other publicly accessible data.

[Dr. Latanya Sweeney](#), who runs Harvard’s Data Privacy Lab, shows how the [mapping of personal health information](#) and other sensitive data has become more complex in the last two decades. She’s demonstrated with multiple projects how [one can re-identify patients without explicit identifiers](#).

You can get stuck in the weeds with this [FERPA versus HIPAA flowchart](#) created by the [Oregon Community Health Information Network](#). The distinctions are not just technicalities as [states like Illinois are grappling with the implications](#). Whether SBHC records are subject to HIPAA or FERPA privacy protections depends on the relationship between the school-based provider and the educational agency.

[School based health centers \(SBHC\)](#) are a fast growing initiative in all states. A place for primary medical care; mental/behavioral health care; dental/oral health care; health education and promotion; substance abuse counseling; case management; and nutrition education. SBHCs are intended to reduce health inequities and improve health outcomes for underserved youth. Between 2010-13, the [Affordable Care Act allocated \\$200 million](#) to improve and expand these services.

Nationally, [only 20% of SBHCs receive funding through the Health Resources and Services Administration](#). 50 of Oregon’s 68 state-certified SBHCs are [federally qualified health centers](#). Federally qualified health centers are [covered entities](#) and must be HIPAA compliant, but do HIPAA *privacy* rules always apply?

Virginia Garcia is a [federally qualified health center](#) (FQHC) that now operates SBHCs in eight school districts. In 2008, the Tigard-Tualatin School District School Board signed a [memorandum of understanding with Virginia Garcia as an SBHC, “completely independent of the district.”](#) Presumably electronic records meet HIPAA standards for *both* security and privacy.

The [newest Virginia Garcia SBHC](#) opened at Beaverton High School. It will eventually serve all students in the Beaverton School District.

[Another SBHC](#) operating in the BSD since 1994 is located at [Merlo Station High School](#). It is “run by the OHSU School of Nursing *within the Beaverton School District’s guidelines* and with support and input from the Washington County Health Department.” The majority of students receiving care there are Hispanic and Community High Students. Teenagers receive prenatal

and postpartum care; and young mothers can get onsite day care at Merlo Station. This SBHC is affiliated with the two Coordinated Care Organizations serving Washington County.

Both of these SBHCs presumably comply with HIPAA security rules. The Beaverton School District School Board has [no written policies and regulations regarding SBHCs](#). Are they run independently of the school district? If not, does the Beaverton School District maintain SBHC health records as *education* records?

When SBHC medical providers disclose information to a *district*-employed school nurse, the data trails become complex. If school nurses maintain [student health records \(including immunization and school nurse records\)](#), they are education records and FERPA regulates student privacy.

Schools use a student information system (SIS) to maintain education records. Most Oregon schools use [Edupoint's Synergy](#). Like an octopus, Synergy has tentacles that reach far beyond test scores. Synergy "archives and displays health history for easy access throughout each student's district career." [Pearson Power School](#) (another SIS) partners with independent health and immunization software vendors.

How long these private companies hold education records and whether or not the data can be re-purposed or shared is buried in terms of use agreements that parents and students cannot readily access.

Education records are uploaded to a [state longitudinal data system](#). Certainly, a student's mental and physical health contributes to success/failure in the preschool through college trajectory. Oregon's longitudinal data system (SLDS) includes vaccinations and tracks students on individual education programs.

Children with disabilities on Individual Education Plans take assessments that overlap into clinical medicine. [Pearson Clinical](#) has the monopoly on these assessments. Whether or not IEP information (such as the IDEA indicator) is included in the SLDS depends on which [data elements](#) the Oregon Department of Education chooses to track.

Telemedicine, a health service delivered through a two-way video communication, would be particularly attractive for school-based health centers. Oregon is on the fast track to pass a [telemedicine bill](#). The [telemedicine reimbursement expansion work group](#) that supports the bill included Michael Tynan representing the School-based Health Program, OHA, and Public Health. (Ted Conklin representing Lifewise-Premera Blue Cross also participated. Premera Blue Cross, if you recall, doesn't have a great track record with personal health information.)

The standards and specifications of the HIPAA Security Rule are specific to electronic protected health information. [E-PHI](#) *“would not include “paper-to-paper” faxes, or person-to-person telephone calls, video teleconferencing, or messages left on voice-mail.”* That means businesses can sell “HIPAA compliant” software to unsuspecting clinicians that is neither since the HIPAA Security Rule doesn’t apply.

[Psychiatric Times](#) reviewed the perils of using Skype. They note that video-chat platforms were developed for marketing to the general consumer, and not for health care. Neither federal nor state law regulates specific proprietary entities such as Skype and its competitors while HIPAA holds professionals responsible for conducting their own internal risk assessments regarding their chosen technologies.

The Center for Telehealth and e-Health Law created a sample videoconferencing consent form that warns of “risks and consequences from use of these services” including “the transmission of my health information could be intercepted or accessed by unauthorized persons.” That’s one way to absolve businesses and clinicians of a responsibility to assure telemedicine is delivered privately.

Students shouldn’t be second-class citizens when their health care is through schools.

Oregon legislators should make amends for U. of O's Wikipedia reputation. HB 3476, while commendable, would deny a college’s legal defense team access to mental health records of domestic violence, sexual assault and stalking victims.

The problem is rooted in FERPA and HIPAA. FERPA's original intent is undermined when education records include health records. Loosening disclosure through FERPA and HIPAA rule changes has accommodated a digital economy, but at great risk to all students.

While Congress is beginning to respond to parents concerned about student data privacy, there is surprisingly little being done to address health data privacy despite the massive data breaches this year. The Oregon legislature should pass a resolution asking Congress to address the failures of FERPA and HIPAA in protecting confidential data.

- Oregon House [Bill 3476](#) should:
 - o Limit health data in education records to vaccines; and

- o Require all public schools to become a “[hybrid entity](#),” designating the health unit (including the school-based health center) as a “health care component”. This separate legal entity would follow HIPAA privacy and security rules.
- The Oregon legislature should create a [Privacy and Security Information Center](#) and hire a Chief Privacy Officer similar to what Ohio has done
- The Oregon legislature should pass bills championed by Rep. Lew Frederick that protect student privacy: [HB 2708](#), [HB 2709](#), [HB 2710](#), [HB 2711](#), and [HB 2712](#); and bills that assure better communication with family members and outpatient management for all individuals suffering with mental illness: [HB 2022](#), [HB 2023](#) and [HB 2948](#)
- The House should not pass [SB 144A](#) without amendments that stipulate telemedicine shall comply with the HIPAA Security Rule and that guidelines for encryption are established.

Thank you!

Kris Alman MD