Testimony of David Fidanque, Executive Director
In Support of HB 2551
House Health Care Committee
March 23, 2015

Chair Greenlick and Members of the Committee:

I am David Fidanque, Executive Director of the ACLU of Oregon and we are pleased to support HB 2551. In essence, the bill would require all covered entities except health care clearinghouses to submit an annual audit report to DCBS or OHA/DHS, demonstrating compliance with federal and state health privacy laws.

Recent announcements of massive data breaches from Anthem and Promera involved the records of as many as 90 million Americans. Anthem, which manages Blue Cross plans in 14 states, is the second largest insurer in the country. Although hackers gained access to Anthem's database beginning last May, the breach wasn't discovered until late January and was announced publicly in early February.

Of course, Oregon is not one of the states served directly by Anthem, but I personally received a letter just last week about the Anthem breach because I am covered by Regence here and had an unscheduled stop at an emergency room in Denver last May. I am just one of about 79 million Blue Cross individuals whose name, date of birth, insurance ID, Social Security number, home address and e-mail address may have been disclosed to the hackers.

Another 11 million people may be impacted by the Promera hack, and that one reportedly also disclosed health care information as well as personal identifying information.[1]

HB 2551 will not solve all of the problems that we face in regard to health privacy, but it is an important step forward to ensure that the safeguards that exist in current law are implemented, monitored, and effective. An audit and a public report will not only compel the auditing entity to examine any weaknesses in the way it collects, stores, and shares information, but will allow the public to inform themselves of the security of their very personal information.

We would like to suggest to the members of the Committee that you might consider including "business associates" in the reporting requirement. As defined in the HIPAA Privacy Rules, a business associate is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[2] Business associates obtain and share private medical records as do covered

[1] Also see attached article, "2015 is already the Year of the Health-Care Hack – And It's Only Going to Get Worse," by Andrea Peterson, Washington Post, March 20, 2015, available at: http://www.washingtonpost.com/blogs/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse/
[2] See http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

entities and should be required to report on the effectiveness of their security measures in the same way.

The issues of privacy of health information are not only complex, but are sometimes perceived to be at odds with coordinated health care delivery. We thank the proponents for raising these issues and proposing immediate and practical solutions to help address them.

Thank you for your consideration.