

March 13, 2015

Representative Ann Pugh, Chair, Vermont House Committee on Human Services

### **Testimony ~ H.98**

Dear Honorable Representative Pugh,

The Vermont Coalition for Vaccine Choice (VCVC) is a volunteer organization dedicated to preserving health choice and informed consent for parents and all Vermonters. We are active community members and a vital part of the Vermont economy: the young families that are the future of Vermont, as well as grandparents, teachers, nurses, healthcare providers, lawyers and others.

Thank you for your consideration of our concerns regarding H.98.

We have three major issues with H.98. The first is that the proposed expansion of the Immunization Registry calls for the collection of adult data as well as student data. The second is that privacy issues and security breaches are, unfortunately, not uncommon, costly and jeopardize personal information. Lastly, everyone is entitled to the same rights and protection of privacy and security of information regardless of disease type or tracking of care.

1) The proposed expansion of the Immunization Registry includes tracking of adult vaccination data. H.98 would require the Vermont Department of Health to obtain, store, and track every Vermonter's vaccination status, not just the status of school children. There is no legal basis for the state of Vermont to track or ensure that Vermont adults are up-to-date on their vaccinations. The current registry was designed for students who have school-entry requirements for vaccines. The inclusion to require adult vaccine data, especially with no opt-out ability, is legal overreach and an unwarranted infringement on personal health privacy. We respectfully ask that the adult vaccine tracking requirement be dropped from the proposed bill.

2) Data breaches are regrettably a serious technological problem. Personal and health information are sensitive and must be protected from unauthorized disclosure. Unfortunately, neither government nor commercial organizations have proved themselves trustworthy when it comes to protecting private personal information. Hardly a week goes by without another data breach of such information. The New York Times recently reported, "Medical identity theft is on the rise, experts say, because it pays. In black-market auctions, complete patient medical records tend to fetch higher prices than credit card numbers." As a result, Bert Reese, CIO of Sentara, a healthcare organization, stated, "We see about a million hits a day from China alone trying to break into our network." Few organizations are prepared for these attacks, according to security firm SANS-Norsk. In a recent report they detailed how healthcare organizations of all types have been and continue to be compromised by successful attacks.

The costs of healthcare data breaches are high for both patients and organizations. The Ponemon Institute, which conducts information security research, recently released their annual report on healthcare data breaches for 2014. They found that once someone becomes a victim of medical identity theft it's extremely difficult, time-consuming, and costly to resolve the problem. Medical identity thieves can rack up thousands of dollars in unauthorized bills and

have their care added to the victims' health records. Victims end up paying an average of over \$13,000 in fraudulent bills.

States dealing with data breaches include Texas, with a Federal regulations violation concerning its 2 million Medicaid records; the state of Montana's Department of Public Health and Human Services had a database hacked that affected all 1 million of the state's residents at a cost to the state of \$2 million; New York City Health & Hospitals Corporation's North Bronx Healthcare Network had 1.7 million records stolen; and the Anthem Health Insurance company recently had 80 million or more records hacked, with a potential cost of \$8-16 billion. All told, the top 10 healthcare data breaches of the last five years exposed the records of over 100 million people to identity theft and cost organizations an estimated \$9.3 to 17.4 billion dollars.

We submit that the potential risks and costs to the state and to residents of maintaining such a database as a vaccination tracking system are not worth the potential benefits, and as in point number one, ask that at the least, the adult vaccine tracking be dropped from the proposed bill.

3) While we question the overall security of any of the registries, we find that the privacy and security requirements in H.98 are inconsistent between each of the three registries. Privacy rules should be consistent regardless of what data, care or diseases are being tracked. We respectfully submit that the thoughtful and appropriate privacy and security measures delineated for the HIV/AIDS registry be applied to all three of the registries covered in H.98.

To this end we suggest that under both the Cancer Registry and Immunization Registry the following language be inserted (taken from the HIV/AIDS registry section):

**Cancer Registry:**

Public health records developed or acquired by State or local public health agencies that relate to Cancer and that contain either personally identifying information or information that may indirectly identify a person shall be confidential and only disclosed following notice to and written authorization from the individual subject of the public health record or the individual's legal representative.

(e) Any person who willfully or maliciously discloses the content of or breaches confidentiality in relation to any confidential public health record other than as authorized by law or in violation of this section shall be subject to a civil penalty of not less than \$10,000.00 and not more than \$25,000.00, costs and attorney's fees as determined by the court, compensatory and punitive damages, or equitable relief, including restraint of prohibited acts, costs, reasonable attorney's fees, and other appropriate relief.

A person committing an act subject to a civil penalty under this section shall also be liable to the subject for all actual damages, including damages for any economic, bodily, or psychological harm that is a proximate result of the act.

The Department shall annually evaluate the systems and confidentiality procedures developed to implement networked and non-networked electronic reporting, including system breaches and penalties for disclosure to State personnel. The Department shall provide the results of this evaluation on its Website.

Immunization Registry:

Public health records developed or acquired by State or local public health agencies that relate to Vaccinations and that contain either personally identifying information or information that may indirectly identify a person shall be confidential and only disclosed following notice to and written authorization from the individual subject of the public health record or the individual's legal representative.

(e) Any person who willfully or maliciously discloses the content of or breaches confidentiality in relation to any confidential public health record other than as authorized by law or in violation of this section shall be subject to a civil penalty of not less than \$10,000.00 and not more than \$25,000.00, costs and attorney's fees as determined by the court, compensatory and punitive damages, or equitable relief, including restraint of prohibited acts, costs, reasonable attorney's fees, and other appropriate relief.

A person committing an act subject to a civil penalty under this section shall also be liable to the subject for all actual damages, including damages for any economic, bodily, or psychological harm that is a proximate result of the act.

The Department shall annually evaluate the systems and confidentiality procedures developed to implement networked and non-networked electronic reporting, including system breaches and penalties for disclosure to State personnel. The Department shall provide the results of this evaluation on its Website under Immunization Surveillance.

In addition, on Page 13 under sections (c) and (d) of the Immunization Registry section we ask that the language again be consistent and reflect the above noted privacy and security provisions by adding the underlined language. Our preference would be that section (d) be deleted in its entirety. Short of that, then amended with the following underlined addition:

(c) The Department may exchange confidential registry information with the immunization registries of other states in order to obtain comprehensive immunization records with written authorization from the individual.

(d) The Department may provide confidential registry information to health care provider networks serving Vermont patients and, with the approval of the Commissioner, to researchers who present evidence of approval from an institutional review board in accordance with 45 C.F.R. § 164.512 with written authorization from the individual.

Again, thank you for your time and consideration.

Respectfully submitted,

Jennifer R. Stella

VT Coalition for Vaccine Choice, (802) 917 3230

Attachments: references and data breach chart

## REFERENCES

- Reed Abelson and Julie Creswell. "Data Breach at Anthem May Forecast a Trend." The New York Times, Feb. 7, 2015. <[http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html?\\_r=1](http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html?_r=1)>.
- Even Schuman. "Top healthcare CISOs hard to come by." Healthcare IT News, May 20, 2014. <<http://www.healthcareitnews.com/news/top-healthcare-cisos-hard-come>>.
- Barbara Filkins. "SANS Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon." SANS Institute, Feb. 2014. <<http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf>>.
- Ponemon Institute. "Fifth Annual Study on Medical Identity Theft." Medical Identity Theft Fraud Alliance, Feb. 2015. <<http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/>>.
- Larry Ponemon. "2014 Cost of Data Breach Study: United States." Ponemon Institute and IBM, May 2014. <<http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/>>.
- Brian Krebs. "Data Breach at Health Insurer Anthem Could Impact Millions." KrebsonSecurity.com, Feb. 4, 2015. <<http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/>>.
- Corey Noles. "Anthem data breach could cost company billions." St. Louis Business Journal, Feb. 13, 2015. <<http://www.bizjournals.com/stlouis/blog/health-care/2015/02/anthem-data-breach-could-cost-company-billions.html?page=all>>.
- Stephanie Goodman. "State Sues Xerox over Failure to Return, Protect Client Data." Texas Health and Human Services Commission, Aug. 26, 2014. <<http://www.hhsc.state.tx.us/news/release/2014/082614-state-sues-xerox.shtml>>.
- Privacy Rights Clearinghouse. "Chronology of Data Breaches Security Breaches 2005 - Present." PrivacyRights.org, Dec. 31, 2013. <<https://www.privacyrights.org/data-breach>>.
- Health Data Management. "10 Top Health Data Hacks." HealthDataManagement.com, accessed Mar. 2, 2015. <<http://www.healthdatamanagement.com/gallery/10-top-health-data-hacks-49763-1.html>>.
- Jeremy Kirk. "Montana data breach exposed 1.3 million records." PCWorld.com, June 24, 2014. <<http://www.pcworld.com/article/2367780/montana-data-breach-exposed-13-million-records.html>>.
- U.S. Health & Human Services Office for Civil Rights. "Breaches Affecting 500 or More Individuals." HHS OCR Complaint Portal, accessed Mar. 2, 2015. <[https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)>.
- Bob Brewin. "TRICARE directs SAIC to offer credit monitoring for data theft patients." Nextgov.com, Nov. 7, 2011. <<http://www.nextgov.com/health/2011/11/tricare-directs-saic-to-offer-credit-monitoring-for-data-theft-patients/50078/>>.
- Dan Munro. "Assessing The Financial Impact Of 4.5 Million Stolen Health Records." Forbes.com, Aug. 24, 2014. <<http://www.forbes.com/sites/danmunro/2014/08/24/assessing-the-financial-impact-of-4-5-million-stolen-health-records/>>.
- Infinity Technologies. "Four Million Patient Records Breached During Burglary at the Advocate Medical Group The Penalty? \$960,000.00." IT-VA.com, accessed Mar. 2, 2015. <<http://blog.it-va.com/blog/four-million-patient-records-breached-during-burglary-at-the-advocate-medical-group-the-penalty-960000-00.html>>.

### Top 10 Health Record Data Breaches in the US 2010-2015

Company	Date	Number	Estimated Cost	Type	Information Exposed	References
Anthem Health Insurance	12/2014-01/2015	80,000,000	\$8-16 billion	Hack	Names, dates of birth, Social Security numbers, addresses, phone numbers & employment information	<a href="http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/">http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/</a> <a href="http://www.bizjournals.com/stlouis/blog/health-care/2015/02/anthem-data-breach-could-cost-company-billions.html?page=all">http://www.bizjournals.com/stlouis/blog/health-care/2015/02/anthem-data-breach-could-cost-company-billions.html?page=all</a>
SAIC	9/13/11	4,900,000	\$148 million+	Theft	Names, Addresses, Personal health information, Phone numbers & Social Security numbers	<a href="https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf">https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf</a> <a href="http://www.nextgov.com/health/2011/11/tricare-directs-saic-to-offer-credit-monitoring-for-data-theft-patients/50078/">http://www.nextgov.com/health/2011/11/tricare-directs-saic-to-offer-credit-monitoring-for-data-theft-patients/50078/</a>
Community Health Systems Professional Services Corp	04/10/2014 - 06/24/2014	4,500,000	\$75-150 million	Hack	Names, addresses, birth dates, telephone & social security numbers	<a href="https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf">https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf</a> <a href="http://www.forbes.com/sites/danmunro/2014/08/24/assessing-the-financial-impact-of-4-5-million-stolen-health-records/">http://www.forbes.com/sites/danmunro/2014/08/24/assessing-the-financial-impact-of-4-5-million-stolen-health-records/</a>
Advocate Medical Group	8/28/13	4,000,000	\$960 million	Theft	Names, Social Security numbers, addresses, dates of birth diagnoses, medical record numbers, medical service codes & health insurance information	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a> <a href="http://blog.it-va.com/blog/four-million-patient-records-breached-during-burglary-at-the-advocate-medical-group-the-penalty-960000-00.html">http://blog.it-va.com/blog/four-million-patient-records-breached-during-burglary-at-the-advocate-medical-group-the-penalty-960000-00.html</a>
Xerox State Healthcare (Texas Medicaid contractor)	5/9/14	2,000,000	\$1 million+	HIPAA violation	Names, photographs, birthdates and medical & billing records	<a href="http://www.hhsc.state.tx.us/news/release/2014/082614-state-sues-xerox.shtml">http://www.hhsc.state.tx.us/news/release/2014/082614-state-sues-xerox.shtml</a>
Health Net	3/15/11	1,900,000	\$114 million+	Loss	Names, addresses, health information, Social Security numbers, health information & financial information	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a>
New York City Health & Hospitals Corporation's North Bronx Healthcare Network	2/12/11	1,700,000	Unknown	Theft	Names, Social Security numbers, addresses, patient health information and other patient & employee information	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a>
Nemours Foundation	10/7/11	1,600,000	Unknown	Loss	Names, Social Security numbers, addresses, dates of birth, insurance information, medical treatment information, direct deposit bank account information & payroll information of current and former employees	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a>
AvMed Health Plans	2/10/10	1,220,000	\$3 million	Theft	Names, addresses, phone numbers, Social Security numbers & protected health information	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a>
Montana Department of Public Health and Human Services	5/29/14	1,062,509	\$2 million	Hack	Patient names, addresses, birth dates & Social Security numbers & employee names, SSNs & bank account numbers	<a href="https://www.privacyrights.org/data-breach">https://www.privacyrights.org/data-breach</a> <a href="http://www.healthdatamanagement.com/gallery/10-top-health-data-hacks-49763-1.html">http://www.healthdatamanagement.com/gallery/10-top-health-data-hacks-49763-1.html</a> <a href="http://www.pcworld.com/article/2367780/montana-data-breach-exposed-13-million-records.html">http://www.pcworld.com/article/2367780/montana-data-breach-exposed-13-million-records.html</a>
<b>TOTALS</b>		102,882,509	\$9.3-17.4 billion			