**“SOMEBODY’S WATCHING ME”**

SESSION DESCRIPTION:

**1:30 p.m. – 3:00 p.m. Somebody's Watching Me**

I always feel like *somebody's watchin' me* might be a one hit wonder from the 80's, but in all reality data privacy and HIPAA reform are hot topics. The Senate Committee on Health, Education, Labor, and Pensions (HELP Committee) released a request for information in September 2023 asking interested parties to provide responses to a spectrum of questions on health data privacy. As technology proliferates and health data interoperability increases, there is greater opportunity to improve care and patients’ access to their health information. Yet, increased access can lead to increased vulnerability for inappropriate data disclosures and a greater pool of data for hostile actors to exploit for nefarious purposes.[[1]](#footnote-2) In 2020, the National Conference of State Legislatures (NCSL) created a Privacy Work Group to examine a range of policy issues, including consumer data privacy, algorithms and artificial intelligence, government data usage, transparency, big data, law enforcement issues, and intersections between data privacy and cybersecurity. To date 13 states and 137 countries have passed data privacy laws while 17 additional states are actively discussing. This roundtable will explore trends organizations should keep a watchful eye on to ensure future legislation and regulation doesn’t have a negative impact.

**DISCUSSION OUTLINE:**

1. (Michele) As a technology company, how do you protect consumer data, especially in light of the fact that Workers’ Compensation and PIP Auto are considered to be “exempt” from HIPPA?
2. (Michele) How do you operate in multiple states, given that each state may have different privacy laws? How can you ensure that you are even able to administer a claim, given all of the consumer data protection restrictions?
	1. Discussion of *Schiff* case in WA
	2. Interoperability (what federal developments have occurred?)
3. (Chris) Can you tell us about on-going litigation that you have seen in this area?
	1. Discussion of IL biometric suits
	2. Class action lawsuit just filed in IL against Target for collecting biometric information
	3. Discussion of **consent** related issues, especially with PEO’s/staffing companies
	4. How do you go about determining *damages* in these suits? What factors do you need to consider? How do you valuate your “fingerprints floating around out there”?
4. Outdated medical forms
	1. The UB-04 has not been updated since 2004!
		1. HI TECH act, use of SSN’s
5. AI use in healthcare – state task forces are looking at how to handle the privacy-related issues
	1. What rights do you have as a consumer over your own data?
	2. What is your right (if any) to privacy or compensation if there’s a breach?
	3. What happens to your data when you DIE?
6. (James) AAPAN members, this is how YOU can get involved…
	1. Discussion of SB2 in CT
		1. Link to legislation: <https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00002&which_year=2024>
		2. Bill summary: To: (1) Establish requirements concerning the development, deployment and use of certain artificial intelligence systems; (2) establish an Artificial Intelligence Advisory Council; (3) prohibit dissemination of certain synthetic images; (4) prohibit distribution of, and agreements to distribute, certain deceptive media concerning elections; (5) require state agencies to study potential uses of generative artificial intelligence and propose pilot projects; (6) require the Commissioner of Administrative Services to provide training concerning generative artificial intelligence; (7) require the Chief Workforce Officer to (A) incorporate artificial intelligence training into workforce training programs, and (B) design a broadband outreach program; (8) require the Board of Regents for Higher Education to establish (A) a "Connecticut Citizens AI Academy", and (B) certificate programs in fields related to artificial intelligence; and (9) require the Department of Economic and Community Development to (A) develop a plan to offer high-performance computing services, (B) establish a confidential computing cluster, and (C) conduct a "CT AI Symposium".
	2. Discussion of IL SB3080 (Health Care Privacy)
		1. Link to legislation: <https://www.ilga.gov/legislation/BillStatus.asp?DocNum=3080&GAID=17&DocTypeID=SB&SessionID=112&GA=103>
		2. Bill summary: **Creates the Protect Health Data Privacy Act.** Provides that a regulated entity shall disclose and maintain a health data privacy policy that clearly and conspicuously discloses specified information. Sets forth provisions concerning health data privacy policies. Provides that a regulated entity shall not collect, share, or store health data, except in specified circumstances. Provides that it is unlawful for any person to sell or offer to sell health data concerning a consumer without first obtaining valid authorization from the consumer. Provides that a valid authorization to sell consumer health data must contain specified information; a copy of the signed valid authorization must be provided to the consumer; and the seller and purchaser of health data must retain a copy of all valid authorizations for sale of health data for 6 years after the date of its signature or the date when it was last in effect, whichever is later. *Sets forth provisions concerning the consent required for collection, sharing, and storage of health data. Provides that a consumer has the right to withdraw consent from the collection, sharing, sale, or storage of the consumer's health data*. Provides that it is unlawful for a regulated entity to engage in discriminatory practices against consumers solely because they have not provided consent to the collection, sharing, sale, or storage of their health data or have exercised any other rights provided by the provisions or guaranteed by law. Sets forth provisions concerning a consumer's right to confirm whether a regulated entity is collecting, selling, sharing, or storing any of the consumer's health data; a consumer's right to have the consumer's health data that is collected by a regulated entity deleted; prohibitions regarding geofencing; and consumer health data security. Provides that any person aggrieved by a violation of the provisions shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. Provides that the Attorney General may enforce a violation of the provisions as an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. Defines terms. Makes a conforming change in the Consumer Fraud and Deceptive Business Practices Act.
1. https://www.help.senate.gov/imo/media/doc/privacy\_report.pdf [↑](#footnote-ref-2)