



Consumer Data Privacy Alignment with Existing Health Privacy Protections

Background

Bills proposing to regulate how businesses process an individual's personal data, including their personal health information (PHI), could apply to hospitals. "Consumer privacy" bills aim to increase consumers' access and control of their personal data and would require several measures toward that end. For instance, the bills would give consumers the ability to "opt-in" or "opt-out" to the processing of their data, as well as impose security and compliance obligations on businesses.

WSHA Position

WSHA supports increasing people's access to and control of their personal data, but we need to ensure state law does not create competing compliance obligations or add burdensome requirements over and above the high standards hospitals already meet as "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA), among other state and federal privacy laws and regulations.

Key Messages

- Hospitals currently protect PHI according to HIPAA standards, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH). These standards address the confidentiality, security and transmissibility of a person's PHI. Patient consent, access and control are central tenets of the law. These are stringent standards, and they should be.
- Hospitals also protect health care related information pursuant to several other state and federal laws and regulations.
- These "same but different" laws would introduce competing requirements, making compliance extremely difficult and draining limited time and resources away from hospitals' existing efforts to protect people's personal data.

Contact Information

Cara Helmer
Policy Director, Legal Affairs
CaraH@wsha.org | 206.577.1827

Lisa Thatcher
WSHA Lobbyist
LisaThatcher@comcast.net | 253.686.8746