

**TESTIMONY OF
CONNECTICUT HOSPITAL ASSOCIATION
PUBLIC HEALTH COMMITTEE
Friday, February 17, 2017**

**SB 447, An Act Concerning The Bidirectional Exchange Of
Patient Electronic Health Records**

The Connecticut Hospital Association (CHA) appreciates this opportunity to submit testimony concerning **SB 447, An Act Concerning The Bidirectional Exchange Of Patient Electronic Health Records**.

Before commenting on the bill, it's important to point out that Connecticut hospitals provide high quality care for everyone, regardless of ability to pay. Connecticut hospitals are finding innovative solutions to integrate and coordinate care to better serve patients and communities, as well as achieve health equity. These dynamic, complex organizations are working to build a healthier Connecticut. That means building a healthy economy, community, and healthcare system. By investing in the future of Connecticut's healthcare and hospitals, rather than continuing to cut away at them, we will strengthen our economy, put communities to work, and deliver affordable care that Connecticut families deserve.

SB 447 seeks to amend existing law ostensibly to clarify that a hospital's efforts to enable its computer systems to accommodate bidirectional exchange of patient electronic health records, as required in 19a-904c of the Connecticut General Statutes, includes that the hospital should both accept electronic health records from, and send electronic health records to, community healthcare providers – specifically including, but not limited to, diagnostic imaging. SB 447 will cause confusion, and likely put medical record integrity and security at risk.

The bill appears to require a hospital to incorporate electronic health records from community providers into the hospital's legal health record, and also to send all records (including imaging) to community providers, essentially if it is technically possible to do so. Those concepts are not a mere clarification of 19a-904c, which mandates enabling of bidirectional exchange within existing resources. Instead the bill would significantly and substantively expand the record sharing requirements in a manner that is inconsistent with safe cyber practices and with federal laws regarding the integrity and security of medical records.

A hospital is obligated by federal law to assess the security risks inherent in any exchange of electronic health information – and specifically *must* affirmatively manage those identified risks. 45 CFR 164.306. Security is not a single event, and security it is not limited to the transport method being secure when data are sent. Security is far broader than encrypting data in transport, and extends to ensuring the integrity of the data and the protection of all connected systems that could be affected if the data were corrupt or compromised. HIPAA security regulations mandate that providers observe their own security risk management policies and procedures. 45 CFR 164.308. This includes not accepting another provider's records in circumstances in which receipt of such records would compromise the provider's systems or the integrity of its own electronic data. (As a corollary, sending electronic records to community providers who lack the capability to maintain their integrity or security is also ill-advised.)

Hospitals continue to make all reasonable efforts to exchange health information across the care continuum. Community providers' cyber networks, processes, and technologies generally lag behind in the essential security and record integrity features necessary to meet federal law requirements and employed by hospitals. No provider should be encouraged, let alone required, to exchange information in a manner that is inconsistent with the HIPAA Security Rule and related guidance.

Thank you for your consideration of our position. For additional information, contact CHA Government Relations at (203) 294-7310.