CONNECTICUT HOSPITAL ASSOCIATION

TESTIMONY OF
CONNECTICUT HOSPITAL ASSOCIATION
SUBMITTED TO THE
GENERAL LAW COMMITTEE
Tuesday, February 25, 2020

SB 137, An Act Concerning Data Privacy Breaches

The Connecticut Hospital Association (CHA) appreciates this opportunity to submit testimony concerning **SB 137, An Act Concerning Data Privacy Breaches**. CHA opposes the bill, as written.

Before commenting on this bill, it is important to point out that Connecticut hospitals and health systems provide high quality care for everyone, regardless of their ability to pay, and work to improve the health of those who live in our communities. Supporting Connecticut's hospitals strengthens our healthcare system and our economy.

Connecticut law contains a variety of competing laws, rules, and requirements governing data breaches, which are usually focused on different industries, and take into consideration the intricacies of businesses and consumers specific to those industries. Section 36a-701b of the General Statutes is a data breach reporting law under "Title 36a - The Banking Law of Connecticut;" specifically, in chapter 669 of the "Regulated Activities" of banking entities.

SB 137 seeks to clarify data breach reporting requirements that were expanded during the 2019 legislative session and inserted into the budget bill, which became Public Act 19-177. The 2019 changes, which are repeated in SB 137 in a more comprehensive format than in the 2019 version, add categories of data to the banking title's chapter 669 that would trigger a reporting obligation and consumer notifications. For years prior to 2019, this law focused on breaches of financial information, which makes sense in the banking title and chapter.

The expansion of data breach elements that trigger reporting pursuant to Section 36a-701b will now include medical information and medical insurance information, which are both far outside of the financial sector, and are also both already highly regulated data elements under federal HIPAA laws to the extent those laws apply to medical providers and health insurers. These changes conflict with current federal breach and notification rules under HIPAA.

While we understand and support the desire to ensure that businesses are not able to ignore security planning or breaches, it is critical to recognize that healthcare covered entities (both providers and health insurers) are already subject to extensive HIPAA privacy, breach, and

security rules, including express federal laws and rules implemented in 2005 addressing security planning and breach assessment, and breach reporting rules first implemented in 2010 and then augmented in 2013 when the HITECH rules became effective.

HIPAA covered entities, both healthcare providers and health insurers, and their business associates should be exempt from the reporting requirements of section 36a-701b because HIPAA and HITECH already include significant security and breach compliance requirements. If these entities are not exempted from the mixed reporting obligations, the result will be substantial confusion for patients and enrollees who will receive multiple, competing, and inconsistent notices about the same incidents. State law should not apply this state banking law to healthcare entities that already must follow long-standing HIPAA reporting obligations designed specifically for the healthcare industry and healthcare consumers.

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