CONNECTICUT HOSPITAL ASSOCIATION

TESTIMONY OF
CONNECTICUT HOSPITAL ASSOCIATION
SUBMITTED TO THE
GENERAL LAW COMMITTEE
Thursday, January 28, 2021

HB 5310, An Act Concerning Data Privacy Breaches

The Connecticut Hospital Association (CHA) appreciates this opportunity to submit testimony concerning **HB 5310, An Act Concerning Data Privacy Breaches**. CHA supports the bill with modifications.

Before commenting on this bill, it is important to acknowledge that, since early 2020, Connecticut's hospitals and health systems have been at the center of the global public health emergency, acting as the critical partner in the state's response to COVID-19. Hospitals expanded critical care capacity, stood up countless community COVID-19 testing locations, and are a critical component of the vaccine distribution plan. Through it all, hospitals and health systems have continued to provide high-quality care for everyone, regardless of ability to pay. This tireless commitment to the COVID-19 response confirms the value of strong hospitals in Connecticut's public health infrastructure and economy and reinforces the need for a strong partnership between the state and hospitals.

HB 5310 is designed to improve awareness for end users and promote transparency for digital information security, particularly for circumstances where bad actors have compromised or breached data systems and digital accounts. The bill adds more specificity and clarity to existing breach notification laws. Unfortunately, even the most sophisticated data systems are vulnerable to intrusion when attacked by motivated bad actors. We are hopeful that federal authorities and data developers can devise more effective ways to block these intrusions. Until those enhanced security mechanisms are ubiquitous, one of the tools available to limit the damage that can be caused by these intrusions is to make end users aware of possible security concerns when they are detected so that they can be more vigilant and take steps to remediate consequences.

As healthcare providers, our member hospitals and their system partners have operated in a highly regulated information security environment since 2005, when the Health Information Portability and Accountability Act (HIPAA) Security Rule first become effective, and we continue to lead in this area. Our hospitals and health systems support the common sense changes in the bill that will clarify when and how to alert individuals when their data may have been compromised. We applaud the leadership of the Office of the Attorney General, and appreciate other stakeholders' input recognizing the need to provide more structure to the process without disrupting existing notification requirements, including HIPAA mandates.

With respect to the appropriate options for notifying end users of a possible compromise of their account or information, and in order to allow a robust security approach while avoiding unintended interference with low-risk business operations, we ask that the following language be included in the bill:

> (1) In the event of a breach of login credentials under subparagraph (B) of subdivision (2) of subsection (a) of this section, notice to a resident may be provided in electronic or other form that directs the resident whose personal information was breached or is reasonably believed to have been breached to promptly change any password or security questions and answer, as applicable, or to take other appropriate steps to protect the affected online account and all other online accounts for which the resident uses the same user name or email address and password or security question and answer.
>
> (2) Any person that furnishes an email account shall first assess if providing notification directly to the email account that was breached or reasonably believed to have been breached creates an unacceptable security risk, and if so, shall provide notice by another method described in this section or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily accesses the account.

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