



GOVERNOR GREG ABBOTT

March 9, 2026

Executive Commissioner Stephanie Muth  
Texas Health and Human Services Commission  
P.O. Box 13247  
Austin, Texas 78711-3247

Commissioner Jennifer A. Shuford, MD, MPH  
Texas Department of State Health Services  
P.O. Box 149347  
Austin, Texas 78714-9347

Vice Admiral Timothy James "TJ" White, USN (Ret.)  
Chief, The Texas Cyber Command  
National Security Collaboration Center  
506 Dolorosa Street – San Pedro 1 Building  
San Antonio, Texas 78204

Dear Commissioner Muth, Commissioner Shuford, Chief White, and University System Chancellors:

Maintaining Texans' physical security and protecting their personal privacy, especially as it relates to something as important and intimate as personal medical data, is of paramount importance. Recently, the Trump Administration's Cybersecurity and Infrastructure Security Agency (CISA) and the United States Food and Drug Administration (FDA) released a series of notices describing security vulnerabilities found in Chinese-manufactured patient monitoring devices. These risks include the ability of unauthorized actors to access protected health information remotely. These notices confirm the warnings of experts who have elevated the proliferation of Chinese-manufactured smart medical devices across our healthcare system as a serious data privacy concern. I will not let Communist China spy on Texans. State-owned medical facilities must ensure there are safeguards in place to protect Texans' private medical data.

The U.S. Food and Drug Administration has a duty to regulate medical devices before and after entering the market. Once deployed, the FDA continues to monitor medical devices through post-market examination. When risks are identified, including cybersecurity risks, the FDA issues alerts and recommendations to reduce harm. On January 30, 2025, the FDA issued a notice raising *Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication*, in which the FDA warned that certain patient monitors contained vulnerabilities that allow unauthorized access, manipulation of devices, and the exfiltration of sensitive patient data, creating meaningful risks for patients. CISA similarly warned that certain Chinese-manufactured monitors contain a "backdoor" through which the device could be controlled remotely and patient data accessed.

These FDA and CISA notices underscore the need for state agencies and state-owned medical facilities to ensure they are continually operating safe and secure environments as even FDA-regulated devices can introduce

operational and cybersecurity risks if they are not carefully assessed and monitored. Given the cybersecurity concerns raised by the FDA, CISA, and other experts about certain foreign-manufactured and internet-enabled medical devices, I direct that Texas state agencies and all state-owned medical facilities take the following actions:

- Health and Human Services Commission (HHSC), the Department of State Health Services (DSHS), and public systems of higher education shall review all state-owned medical facilities operated under their jurisdiction and attest that all new purchases of medical devices used in state-owned medical facilities were procured in compliance with Executive Order GA-48;
- HHSC, DSHS, and public systems of higher education shall catalog and share their inventory of all state-owned medical devices capable of transmitting data via a network and/or that can be accessed remotely to the Texas Cyber Command (TXCC);
- HHSC, DSHS, and public systems of higher education, with the assistance of TXCC, shall review all cybersecurity policies implemented to protect personal health information at all state-owned medical facilities operated under their jurisdiction. Such reviews must specifically include how policies address alerts and notices issued by the FDA or CISA for internet-connected medical devices;
- HHSC shall promote awareness of FDA resources for reporting cybersecurity concerns with medical devices through an outreach campaign to Texas hospitals and other healthcare providers regulated by HHSC;
- TXCC shall review whether the Contec CMS8000 and Epsimed MN-120 patient monitors, or any other items used by HHSC, DSHS, and public systems of higher education that have been the subject of a FDA safety notice, should be included on Texas' prohibited technology list and make recommendations to the Office of the Governor; and
- TXCC shall convene appropriate executives at HHSC, DSHS, and public systems of higher education to make recommendations for improvements to state agency policies for medical devices to address emergent cybersecurity risks, monitoring of devices, and mitigation strategies.

Addressed agencies shall submit their reports and recommendations on the above directives to the Office of the Governor by April 17, 2026.

In addition to the executive actions above, I will propose legislation next session to protect Texans' medical data from foreign hostile actors like Communist China.

Sincerely,



Greg Abbott  
Governor