



STATE OF FLORIDA

JAMES UTHMEIER
ATTORNEY GENERAL

February 5, 2026

Wayne Quinn, President
Mindray North America
800 MacArthur Boulevard
Mahwah, New Jersey 07430

Dear Mr. Quinn:

Florida shines as a global hub for innovation and commerce, but our openness must not be mistaken for vulnerability. As Attorney General, my primary duty is to protect the safety and security of Florida's citizens. Recent investigations and federal warnings have made it clear that the Chinese Communist Party ("CCP") is actively exploiting commercial channels to infiltrate our critical medical systems and harvest the personal data of Americans.¹

In light of these escalating national security threats, the State of Florida is demanding increased transparency from those operating critical medical devices within our borders.² The CCP's 2017 National Intelligence Law mandates that Chinese companies and individuals cooperate with state intelligence efforts. This draconian requirement creates a permanent backdoor for a foreign adversary to access sensitive information from any entity with ties to the People's Republic of China.

Whether through medical technology, telecommunications, or digital platforms, the risk of data exfiltration is a direct threat to our sovereignty.³ We have already seen instances of Chinese-manufactured devices containing unauthorized backdoors that transmit sensitive biometric and personal information to overseas addresses. Florida will not allow its residents

¹ Robert Schmad, *Espionage-linked Chinese company embedded in top US research labs*, Oct. 12, 2025, [washingtonexaminer.com/news/investigations/3846649/espionage-linked-chinese-company-embedded-us-research-labs/](https://www.washingtonexaminer.com/news/investigations/3846649/espionage-linked-chinese-company-embedded-us-research-labs/); U.S. Food & Drug Administration, *Cybersecurity Vulnerabilities with Certain Patient Monitors from Contec and Epsimed: FDA Safety Communication*, Jan. 30, 2025, [fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication](https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-patient-monitors-contec-and-epsimed-fda-safety-communication).

² Cybersecurity & Infrastructure Security Agency, *Contec CMS8000 Contains a Backdoor*, Jan. 30, 2025, cisa.gov/sites/default/files/2025-01/fact-sheet-contec-cms8000-contains-a-backdoor-508c.pdf.

³ Federal Register, *Notice of Request for Public Comments on Section 232 National Security Investigation of Imports of Personal Protective Equipment, Medical Consumables, and Medical Equipment, Including Devices*, Sept. 26, 2025, [federalregister.gov/documents/2025/09/26/2025-18729/notice-of-request-for-public-comments-on-section-232-national-security-investigation-of-imports-of](https://www.federalregister.gov/documents/2025/09/26/2025-18729/notice-of-request-for-public-comments-on-section-232-national-security-investigation-of-imports-of).

to be monitored or manipulated by hostile actors under the guise of routine business operations.

Florida has passed laws to protect against these threats. Florida requires that electronic health records and patient information must be physically maintained in the United States or Canada.⁴ Florida also prohibits “the state government from contracting with entities owned or controlled by the People’s Republic of China, if, as a result, the entity would gain ‘access to an individual’s personal identifying information.’”⁵ Unauthorized access of data in electronic form containing personal information must be reported in many instances under the Florida Information Protection Act of 2014.⁶ As Florida’s chief law enforcement officer, I will diligently work to ensure that Florida’s laws are followed.

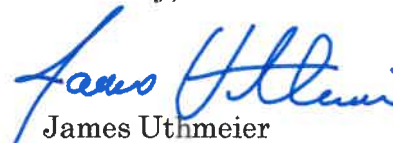
Therefore, this office is demanding a rigorous internal audit and report on the following information to the Office of the Attorney General:

- Disclose any ownership stakes, board memberships, or significant financing provided by the CCP, the Chinese Government (at the central, provincial, and local level), or state-owned or state-controlled entities.
- Confirm if your company or its parent organization is subject to China’s National Security Law, including its provision requiring that businesses under its jurisdiction provide data to Chinese state agencies upon request.
- Report any instance to date in which your company, its parent organization, or its subsidiaries have been asked or compelled by the CCP or by other offices of the Chinese government to share data, proprietary information, or technical specifications regarding operations in China, the US, or other countries.

We must ensure that the products and services used by our families, hospitals, and government agencies are not serving as tools for foreign espionage.

Florida stands ready to defend its citizens. We expect your prompt attention to this critical matter and expect your full cooperation in securing our great state. If you are not inclined to cooperate with this reasonable request, please notify my office where you would like us to send a subpoena formally requesting documents and information under section 501.206(1), Florida Statutes, by February 20th, 2026.

Sincerely,



James Uthmeier
Florida Attorney General

⁴ § 408.051(3), Fla. Stat.

⁵ *Shen v. Comm’r, Fla. Dep’t of Agric. & Consumer Servs.*, 158 F.4th 1227, 1238 (11th Cir. 2025) (quoting § 287.138(2), Fla. Stat.)

⁶ § 501.171, Fla. Stat.