

Author Full Name : JAMES POOLE

Received Date : 04/10/2026 04:55 AM

Comments Received :

This comment supports the continued use of medical history and examination requirements but identifies a critical integrity gap: identity verification associated with these records is not consistently aligned with existing sanctions, export control, and national security screening frameworks.

Medical examination processes rely on verified identity and supporting biographic data. Where these processes are connected to individuals participating in export-controlled environments or activities, identity assurance should be consistent with existing federal screening obligations under:

- 22 CFR § 126.1 (prohibited exports, imports, and sales to certain countries)
- 22 CFR § 126.18 (screening requirements for access to controlled technical data)
- 31 CFR Chapter V (OFAC sanctions programs, including blocked persons and terrorism-related restrictions)
- 31 CFR Chapter X (FinCEN beneficial ownership and anti-money laundering frameworks)
- 15 CFR Parts 744 and 764 (BIS end-use, end-user, and diversion controls under the EAR)
- 19 U.S.C. § 1307 and the Uyghur Forced Labor Prevention Act (CBP import prohibitions tied to forced labor supply chains)

Currently, identity elements associated with medical screening are not required to be validated against these existing enforcement systems. This creates a structural vulnerability where individuals may pass administrative identity checks while remaining associated with sanctioned entities, high-risk jurisdictions, or forced labor-linked supply chains.

Policy clarification is warranted.

First, identity verification associated with medical examination records should be aligned with existing screening practices used for export control and sanctions compliance. This includes validation against restricted party lists, sanctions designations, and other lawful federal screening systems, without expanding the scope of medical data collection.

Second, where individuals are granted access to controlled environments, technical data, or defense-related activities, identity assurance should be consistent with screening requirements under 22 CFR § 126.18, including consideration of affiliations, ownership structures, and jurisdictional risk indicators.

Third, screening processes should account for indirect risk exposure, including intermediary affiliations, beneficial ownership links, and connections to jurisdictions associated with sanctions evasion, terrorism financing, or forced labor production, including Xinjiang-linked supply chains.

Fourth, any integration of identity verification with enforcement systems must be limited to identity confirmation and fraud prevention. Medical data itself should not be used for enforcement analysis and must remain protected consistent with applicable privacy requirements.

Finally, aligning identity verification processes with existing sanctions, export control, and forced labor enforcement frameworks strengthens the integrity of the overall system by preventing unauthorized access, identity fraud, and indirect participation by restricted parties.

This approach preserves the purpose of medical examination requirements while ensuring that identity assurance supports broader national security, sanctions, and supply chain enforcement objectives consistent with existing statutory and regulatory authorities.