AdvaMed* U.S. Health Data Privacy Principles

The collection, sharing and use of health information is fundamental to advancing health care, and holds the promise of delivering higher quality care and better health outcomes at lower overall cost. It is essential that U.S. privacy policy foster continued innovation in health care, while assuring individuals that personally identified data used for health-related purposes ("personal health data") is subject to meaningful privacy safeguards.

People should have a general right to access their personal health data, and those who hold or use personal health data must be responsible stewards of that data, which includes assuring privacy and data security.†

AdvaMed member companies take seriously their obligation to ensure the appropriate use and privacy of personal health data and, where appropriate, minimize privacy concerns by using data from which specific personal identifiers have been removed ("deidentified health data"). Medical technology companies also have a responsibility and an obligation to use personal health data and deidentified health data to comply with existing and evolving regulatory and payment policies and regulations that set forth stringent patient safety, effectiveness, and outcomes-based requirements.

The use of personal health data and deidentified health data in the medical technology field supports health and wellness; aids in the development of diagnostics, treatments and cures; improves health care interventions and outcomes; enables research; drives technology innovation; and enhances the quality and efficiency of health care delivery.

AdvaMed supports a national approach to data privacy that takes into account the unique nature and importance of personal health data and deidentified health data used to advance health care, and commends policymakers for their attention to this important issue.

---

* The Advanced Medical Technology Association (AdvaMed) is the leading trade association representing medical technology manufacturers in the U.S. and around the world. AdvaMed advocates globally for the highest ethical standards and patient access to safe, effective, and innovative medical technologies that save and improve lives.

† Although overlap may exist, policies regarding the use and privacy of health care data should be distinguished and considered separately from policies regarding the protection of data from unauthorized access. See AdvaMed's Medical Device Cybersecurity Foundational Principles. Also see AdvaMed's Guiding Principles on Clinical Trial Data Transparency.

To support continued innovation in health care through the responsible use of personal and deidentified health data, AdvaMed endorses the following principles.

U.S. data privacy policy should:

- Harmonize privacy requirements and standards nationwide to ensure clarity, consistency, predictability, and efficient compliance and oversight, taking into account existing regulatory frameworks for personal health data and deidentified health data.

- Take into account the unique nature and widely varied, complex uses of personal health data and deidentified health data to ensure that their utility is not unduly limited, including with regard to cross-border sharing and use.

- Incorporate a risk-based approach to both personal health data and deidentified health data, such that privacy obligations and protections are proportional to the sensitivity of data and do not unduly constrain important uses of data to improve health care.

- Establish a comprehensive and practical approach to notice and consent regarding the collection and use of personal health data.

- Ensure that individuals have reasonable access to their personal health data from the entity with primary responsibility for the original purpose for which the data was collected.

- Reserve oversight and enforcement to federal authorities with appropriate privacy expertise.