AdvaMed
Advanced Medical Technology Association

1301 Pennsylvania Avenue, NW
Suite 400
Washington, D.C. 20004
P :: 202.783.8700
F :: 202.783.8750
W:: AdvaMed.org

February 14, 2024

Senator Pamela Beidle, Chair
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

Senator Katherine Klausmeier, Vice-Chair
3 East
Miller Senate Office Building
Annapolis, Maryland 21401

RE: Maryland Online Data Privacy Act of 2024 – MedTech Health Privacy Concerns Support with Amendments

Chair Wilson, Vice-Chair Crosby, and Members of the Committee,

AdvaMed appreciates your willingness to support the overall effort to provide confidence to your constituents that their data privacy is secured. SB 541 would provide the residents of Maryland with transparency and control over their personal data and provide new privacy protections. AdvaMed appreciates the opportunity to provide comments regarding SB 541 before the committee to offer support for the bill with two requested amendments that address med tech health privacy concerns.

AdvaMed member companies produce the medical devices, diagnostic products, and digital health technologies (collectively, "Medical Technologies") that are transforming health care through the potential for earlier disease detection, less invasive procedures, and more effective treatments. AdvaMed members range from the largest to the smallest medical technology innovators and companies. We are committed to ensuring patient access to lifesaving and life-enhancing devices and other advanced medical technologies in the most appropriate settings.

AdvaMed champions a **patient-centered framework** for the use and disclosure of health information. AdvaMed believes this can be accomplished by (i) ensuring transparency around the collection, use, and sharing of health information, (ii) ensuring that obtaining consent does not unduly delay or diminish the quality of patient care, and (iii) harmonizing health privacy and security laws and regulations.

AdvaMed Recommendations

AdvaMed recommends the addition of two clarifying provisions that are consistent with the consumer privacy laws adopted in all states to date to avoid negatively impacting patient care and research and development.

Information treated like PHI under HIPAA.

As discussed below, some Health Care Provider (HCP) use of medtech data in patient care is not technically PHI under HIPAA (e.g., the concierge medicine example above). Data from such devices are not exempted under any of the current exemptions of HB 567. Thus, for example, patient data from ultrasounds used by HCPs who are covered recipients under HIPAA is excluded under HIPAA, while patient data from ultrasounds used by concierge physicians is regulated as personal data under the HB 567 even though the manufacturer treats data from both devices in the same way. However, various consumer rights and controller duties that are inconsistent with patient care and regulatory obligations would apply to the data from the concierge physician's ultrasound. Other health care providers that do not conduct HIPAA covered transactions also include free clinics, direct primary care/subscription-based care, cosmetic surgeons, and free-standing cosmetic surgery centers. Data from medical devices used by these other providers that do not accept insurance would similarly fall under the HB 567 regulatory framework instead of HIPAA.

This conflict can be addressed through an exclusion for information treated like PHI collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is disclosed in accordance with HIPAA and afforded all the privacy protections and security safeguards of HIPAA and its implementing regulations. Such a provision could be inserted in § 14-4603 just after § 14-4603(B)(1) exempting PHI under HIPAA as shown below.

> **§ 14-4603.**
>
> . . .
>
> (B) The following information and data are exempt from this subtitle:
>
> (1) Protected health information under HIPAA.
>
> (2) Information treated like protected health information collected, used, or disclosed by a covered entity or business associate under HIPAA when the information is used or disclosed in accordance with HIPAA and the information is afforded all the privacy protections and security safeguards of the federal laws and implementing regulations under HIPAA.
>
> . . .

Unify De-identified Data Definition with HIPAA.

Data de-identified under HIPAA may not be considered "de-identified data" under this bill. Some patient data controlled or processed by medtech companies is de-identified under the HIPAA and transmitted for analysis, research, development, or some other essential health care purpose. AdvaMed recommends adding a clarifying provision so that data de-identified under HIPAA can continue to be used for analysis, private research, and development that can advance scientific understanding and lead to improvements in care and innovative solutions. This can be

accomplished by supplementing the definition of "de-identified data" with an additional sentence, as shown by the blue underlined text below.

§14-4601.

(A) In this subtitle the following words have the meanings indicated.

. . .

(P) "De-identified data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the controller that possesses such data does all of the following:

(1) Takes reasonable measures to ensure that such data cannot be associated with an individual.

(2) Commits in publicly available terms and conditions or in a publicly available privacy policy to maintain and use the information in de-identified form; and

(3) Contractually obliges any recipients of the information to comply with all provisions of this subsection.

"De-identified data" also includes data de-identified in accordance with the requirements in 45 CFR 164 (HIPAA), where any recipients of such data are contractually prohibited from attempting to reidentify such data.

MedTech Privacy Concerns

The medical technology industry is committed, and continues to be highly incentivized, to implement privacy and data security practices that enhance the protection of patients and the quality and reliability of products and services. Unlike companies in other sectors that may focus on collecting and monetizing personal information as their primary commercial objectives, medtech companies use data about patient and health care professional users' experiences to evaluate the safety and effectiveness of potential products, and — if and when cleared or approved for marketing — to support the ongoing legal compliance of products. AdvaMed member companies take seriously the level of trust placed in them by patients and have consistently taken action to self-identify best practices to balance innovation with patient protections.

While transparency is a crucial element of patient-centered health care, requiring specific and potentially repetitive affirmative consent for certain health-related uses is incompatible with our health care ecosystem. It is critical for patient care, device oversight, and the interests of public health that essential uses of patient and health information are not unduly impeded and that legislation be harmonized with existing laws and regulations that permit or require retention of

health-related data for specific purposes (*e.g.*, for treatment, payment, health care operations, research, and FDA-regulatory purposes).

We believe that essential health care- and Medical Technology-related purposes (for which the public interest supports broad data use by Medical Technology companies without repeated affirmative consent for each separate element) ("**Essential Purposes**") include:

- Patient treatment and related activities, including efforts to address equitable access;
- Product monitoring (including safety activities and research to improve safety profiles);
- Research and development;[1]
- Personalized medical device manufacturing/customization (*e.g.*, 3D printed implant or other bespoke device tailored to individualized specifications that requires scans, images, and patient data to be sent to the manufacturer/service provider for customization);
- Product development and improvement (*e.g.*, data is needed by artificial intelligence technologies to train and develop algorithms, and it is unrealistic to back out data from a working algorithm in a cleared product after the fact. It is becoming increasingly clear that reducing bias and developing equitable algorithms will require access to expanded and diverse datasets);
- Regulatory and payer compliance (including evidentiary requirements for coding, coverage, and reimbursement);
- Participation in value-based health care arrangements;
- Ongoing operations (including customer support); and
- Other activities in the interest of the public good, such as contributing to the response to a public health emergency.

Unique MedTech Data Privacy Issues in Patient Care

No Direct Interface with the Patient. In many instances, medtech companies do not directly interface with patients--often, a physician is the individual who selects the device and chooses to use it with certain patients based on their clinical judgment. In certain scenarios, patient data collected by medical devices is not Protected Health Information under HIPAA, as exemplified in the concierge physician example above. Furthermore, some health care providers purchase medtech through third-party distributors. In some of those instances, the medtech company will not have a means of interacting with clinicians to ascertain whether or not they are covered entities under HIPAA. These dynamics pose tension with certain provisions of SB 541.

An affirmative express consent framework is inappropriate for many medical devices used in patient care. While obtaining patient consent may be appropriate for some of these other use cases, requiring specific and potentially repetitive affirmative consent for certain uses related to health care threatens to prove unworkable. This is particularly true given that a

[1] R&D is distinguishable from product development and can lead to advancing medical science and innovative procedures or solutions.

patient may interact with many different Medical Technologies in an instance of acute healthcare need. The burden of obtaining and recording consent would fall on already time-pressed health care professionals to collect individual consent for each device utilized. Requiring specific and potentially repetitive consent for the permutations of data uses that support essential health care purposes is an unworkable approach.

A patient may interact with many different technologies during a single episode of care—vitals, pulse oximetry, *in vitro* diagnostic tests, EKG, echocardiogram, fluoroscopy or other diagnostic imaging, heart monitor, and electronic medical records. Requiring consents specific to each device during an urgent care situation would waste valuable time. In less urgent scenarios, repeated consent could more detrimentally burden the very sick or elderly. That is why Congress adopted a notice framework for HIPAA rather than a consent framework that requires consent for all health- and medtech-related uses of information, which is ill-suited for our health care system. However, some medtech data in patient care is not technically protected health information under HIPAA, since certain providers are not covered entities because they do not engage in HIPAA covered transactions.

Certain Consumer Personal Data Rights Conflict with Other Regulatory Obligations for MedTech
For example, the right to delete personal data obtained about the consumer is inconsistent with data retention requirements for medical records and FDA regulatory requirements.

MedTech Company application of HIPAA protections to data that is not Protected Health Information (PHI) under HIPAA.
The HIPAA regulations apply to "covered entities," including payers and certain health care providers, as well as their "business associates." HIPAA requires covered entities to use risk-based administrative, technical, and physical safeguards to keep protected health information private and secure and outlines specific criteria for when such data may be shared. HIPAA business associates carry out various functions for covered entities and must enter into a HIPAA Business Associate Agreement requiring them to comply with the same HIPAA restrictions that apply to the covered entity.

Some medtech companies treat all patient data in the manner that HIPAA-Covered Entity/Business Associate must treat Protected Health Information.
Medtech companies can be a Covered Entity/Business Associate under HIPAA with regard to certain patients but technically not a HIPAA-regulated entity in relation to other patients. Such companies may choose to handle all patient data from devices in both scenarios as a HIPAA-covered entity should for operational consistency or because they do not have insight into which scenario the patient falls under.

- **Patient Data from MedTech Devices Outside of HIPAA—Concierge Medicine Example.** HIPAA only regulates a Health Care Provider (HCP) when it conducts certain transactions[2] related to health insurance coverage electronically. A concierge physician

[2] 45 C.F.R. 160.103 (Covered entity means . . . (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

who does not accept insurance will not engage in HIPAA-covered transactions (electronic transmissions of patient information related to insurance coverage) and, accordingly, will not be a covered entity under HIPAA. Thus, technically, information from medical devices utilized by such concierge physicians is not protected under HIPAA. However, medtech companies navigating the unique complexity of whether or not HIPAA applies to certain patient data will likely choose to treat all data from such devices as protected under HIPAA out of an abundance of caution and maintain the data in the manner required of covered entities/business associates.

Conclusion

AdvaMed appreciates this opportunity to offer comments. To date, fourteen states have passed their data privacy reform laws that include amendments similar to those requested above. Most recently, New Hampshire passed legislation inclusive of all key healthcare exemptions that allow healthcare delivery, research, and patient privacy to interact and proceed unimpeded. We encourage the committee to follow suit and ensure that there continues to be alignment across the country with respect to data privacy.

Thank you, Chair Beidle and Vice-Chair Klausmeier, for your consideration, and we look forward to working with you and the committee on these amendments. We welcome any opportunity to serve as a resource, especially as it relates to medtech data privacy and security. If you have any questions or need additional information, please contact rkozyckyj@advamed.org.

Respectfully submitted,

. . .

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) Health care claims or equivalent encounter information. (2) Health care payment and remittance advice. (3) Coordination of benefits. (4) Health care claim status. (5) Enrollment and disenrollment in a health plan. (6) Eligibility for a health plan. (7) Health plan premium payments. (8) Referral certification and authorization. (9) First report of injury. (10) Health claims attachments. (11) Health care electronic funds transfers (EFT) and remittance advice. (12) Other transactions that the Secretary may prescribe by regulation.)