ACRO
ASSOCIATION OF CLINICAL RESEARCH ORGANIZATIONS

**STATEMENT OF THE ASSOCIATION OF CLINICAL RESEARCH ORGANIZATIONS**

Introduction

The Association of Clinical Research Organizations (ACRO) represents the world's leading clinical research and technology organizations. Our members provide a wide range of specialized services across the entire spectrum of development for new drugs, biologics and medical devices, from pre-clinical, proof of concept and first-in-man studies through post-approval and pharmacovigilance research. In 2018, ACRO member companies managed or otherwise supported a majority of all FDA-regulated clinical investigations worldwide.

Beyond their work in conducting and facilitating clinical trials, the companies of ACRO regularly use de-identified data (as defined by HIPAA) in the course of post-approval work, including safety surveillance and epidemiology studies, patient registry and health outcomes analyses, comparative effectiveness research (CER), and other information-based research. ACRO members also deploy data analytics tools that are derived from de-identified data to support biopharmaceutical commercialization, pricing and market access decisions, and consult to biopharmaceutical companies, payers and providers in regard to value-based contracts.

With more than 130,000 employees engaged in research activities in every U.S. state and 114 countries around the world, the member companies of ACRO advance clinical outsourcing to improve the quality, efficiency and safety of biomedical research.

ACRO writes in opposition to SB 703, which, if enacted, would do significant damage to clinical and data research and, in our opinion, to the health care system as a whole.

The HIPAA De-identification Regimen Carefully Protects Individual Privacy While Facilitating Health Research

Having worked with the U.S. Department of Health and Human Services and the Office for Civil Rights on issues relating to the research use of health information since our founding in 2002, ACRO notes, first, that the HIPAA Privacy Rule distinguishes between the use of protected health information (PHI) which identifies an individual, and de-identified information for which “there is no reasonable basis to believe that the information can be used to identify an individual” [45 CFR 164.514 (a)].

To use PHI a researcher must, with certain exceptions, obtain an Authorization from the individual, just as he/she must seek the individual’s Informed Consent to participate in a clinical trial to test the safety and effectiveness of a new drug or treatment.

ACRO
ASSOCIATION OF CLINICAL RESEARCH ORGANIZATIONS

Recognizing the enormous promise of health data (now "big data") to improve the health care system, without jeopardizing the privacy of individuals, the HIPAA Privacy Rule does not require the Authorizations of individuals for the creation, use and dissemination of de-identified data, as again "there is no reasonable basis to believe that the information can be used to identify an individual." [We would note that, while successful re-identification attacks against various data sets have been reported, the literature does not describe any successful re-identification of a data set de-identified to the standards established at 45 CFR 164.514 (a)-(c).]

With this careful balance that protects privacy while enabling critical research to proceed, today de-identified data powers a wide variety of research, including: comparative effectiveness studies that help determine optimal treatment approaches; epidemiologic, observational and health trends studies; and, importantly, the creation of data sets that help shape the design of clinical trials and the identification of the kinds of patients who can benefit from inclusion in a trial.

To illustrate the use of de-identified data, today clinical trials of promising treatments can be guided by a reasonable certainty that a requisite number of patients meeting the trial criteria can be found, and near which research centers they live, before the trial even starts. Relying on guesses is too costly, and de-identified 'big data' has empowered CROs and pharmaceutical companies to better design trials with inclusion and exclusion criteria that are not so strict that they overly limit the patient pool or so broad that the population of patients included in the trial will obscure treatment effects. This data also guides where trials are placed, near enough to a sufficient population meeting the criteria. If Oregon adopts SB 703, it is foreseeable that biopharmaceutical companies will avoid placing trials in the state, discouraging researchers and delaying access to promising medicines for Oregon residents.

Further, personalized medicine, which aims to target new treatments precisely for individual patients who will benefit from them, depends upon the very health data sets that SB 703 would limit.

These, and many other kinds of health research, will become significantly hobbled, if not simply made impossible, if individual Authorizations had to be obtained from hundreds of thousands of Oregon patients in order for de-identified data to be created and used in the state.

<u>SB 703 Cannot Pre-empt The De-identification Regimen Of HIPAA Because It Is Not "More Protective" Of Privacy</u>

As drafted, SB 703 asserts that the creation of de-identified data by Covered Entities subject to the HIPAA Privacy Rule is permitted "under limited circumstances and for limited purposes." In fact, no such limitations are found in the relevant sections of the Rule:

- In the definition of *health care operations* at 45 CFR 164.501 (6)(v) –

  "Consistent with the applicable requirements of 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity";

- In the general rules for uses and disclosure at 45 CFR 164.502(d)(1)(2) –

  "(d) *Standard: Uses and disclosures of de-identified protected health information* -

  (1) *Uses and disclosures to create de-identified informati*on. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified information is to be used by the covered entity.

  (2) *Uses and disclosures of de-identified information.* Health information that meets the standard and implementation specifications for de-identification under § 164.514(a) and (b) is considered not to be individually identifiable health information, i.e., de-identified. The requirements of this subpart do not apply to information that has been de-identified in accordance with the applicable requirements of § 164.514, provided that:
  (i) Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of protected health information; and

  (ii) If de-identified information is re-identified, a covered entity may use or disclose such re-identified information only as permitted or required by this subpart."

- And in the standard/implementation specifications at 45 CFR 164.514(a)-(c) –

  "(a) *Standard: De-identification of protected health information.* Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

  (b) *Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if:

  (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

  (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

  (ii) Documents the methods and results of the analysis that justify such determination; or

  (2)

  (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

*(1)* The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

*(2)* The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) *Implementation specifications: Re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:

(1) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification."

Simply, the claim of SB 703 that Covered Entities that are themselves creating, or are disclosing PHI to Business Associates to create de-identified health information, or Covered Entities, Business Associates or other entities that are using and disseminating de-identified data sets are taking an action that in some way violates individual privacy rights or skirts the HIPAA Privacy Rule is not supported.

Because HIPAA is meant to be a floor and not a ceiling for the protection of health privacy, SB 703 could over-ride or pre-empt the provisions of the Privacy Rule cited above if it were "more protective" of individual privacy. But, as noted previously, there has not been any demonstration of privacy harm to individuals caused by the creation, use or dissemination of health data de-identified to a HIPAA standard, so a meaningful case for the bill being somehow "more protective" of privacy appears exceedingly difficult to make.

How does SB 703 aim to over-ride the provisions of the HIPAA Privacy Rule that permit Covered Entities to create, use and disclose de-identified health information? Again, the bill does not purport to protect individual privacy; instead, SB 703 aims to create a property right in relation to an individual's protected health information (PHI). But this property right would exist in relation to one, and only one, use of PHI: to create and disclose de-identified health information. And, even then, the "property" right would apply only if the de-identified data was sold, (and not, for instance, disseminated to a public health agency at cost.) Clearly, the drafters of SB 703 have proposed an extraordinarily attenuated "property right."

Because the creation of de-identified health information is itself privacy-protective, we are astounded that Oregon would contemplate a regimen that would require a new infrastructure that would have to record, monitor, track and communicate about authorizations (or the lack thereof) for every patient in the state. In essence, Covered Entities or Business Associates or new vendors would have to access the PHI of every individual patient – and thereby create a new risk to privacy – in order to obtain a newly required "signed authorization" to permit a Covered Entity to create and disseminate de-identified data, (which we again point out, the Covered Entity is permitted to do under the HIPAA Privacy Rule.) SB 703 would reduce, rather than increase, the privacy of health information – and we strongly doubt that it could prevail if a challenge were brought to its scheme to over-ride Federal law.

SB 703 is not more protective of privacy than the existing HIPAA regimen for the de-identification of health information. Further, SB 703 assumes a health information marketplace that simply does not exist. Its presumption that the de-identified data of a single individual has value is wildly inconsistent with the actual applications, the analytics and tools "built from" de-identified data,

which typically rely on the data from millions of records, that are used to improve care coordination, address the quality and cost of health care, and in a hundred other ways. Its notion that individuals should be able to assert a property right in information that does not identify them, and for which there is no reasonable basis to believe they could be re-identified, strains credulity.

Conclusion

Representing companies whose lifeblood is the collection and analysis of health information to test the safety and efficacy of new drugs and new treatments for patients, ACRO strongly supports the creation and use of de-identified data as a privacy-protective method for unlocking the promise of health data. We are pleased to report that the HIPAA regimen for the creation and use of de-identified data has engendered a research analytics ecosystem that makes use of health data at scale, and protects the privacy of individuals.

In our view, SB 703 is an ill-conceived solution in search of a problem. We urge the Senate Judiciary Committee to not advance the bill.

Respectfully submitted,

Douglas Peddicord, Ph.D.
Executive Director