Ann B. Waldo, JD, CIPP

Waldo Law Offices, PLLC

Vermont

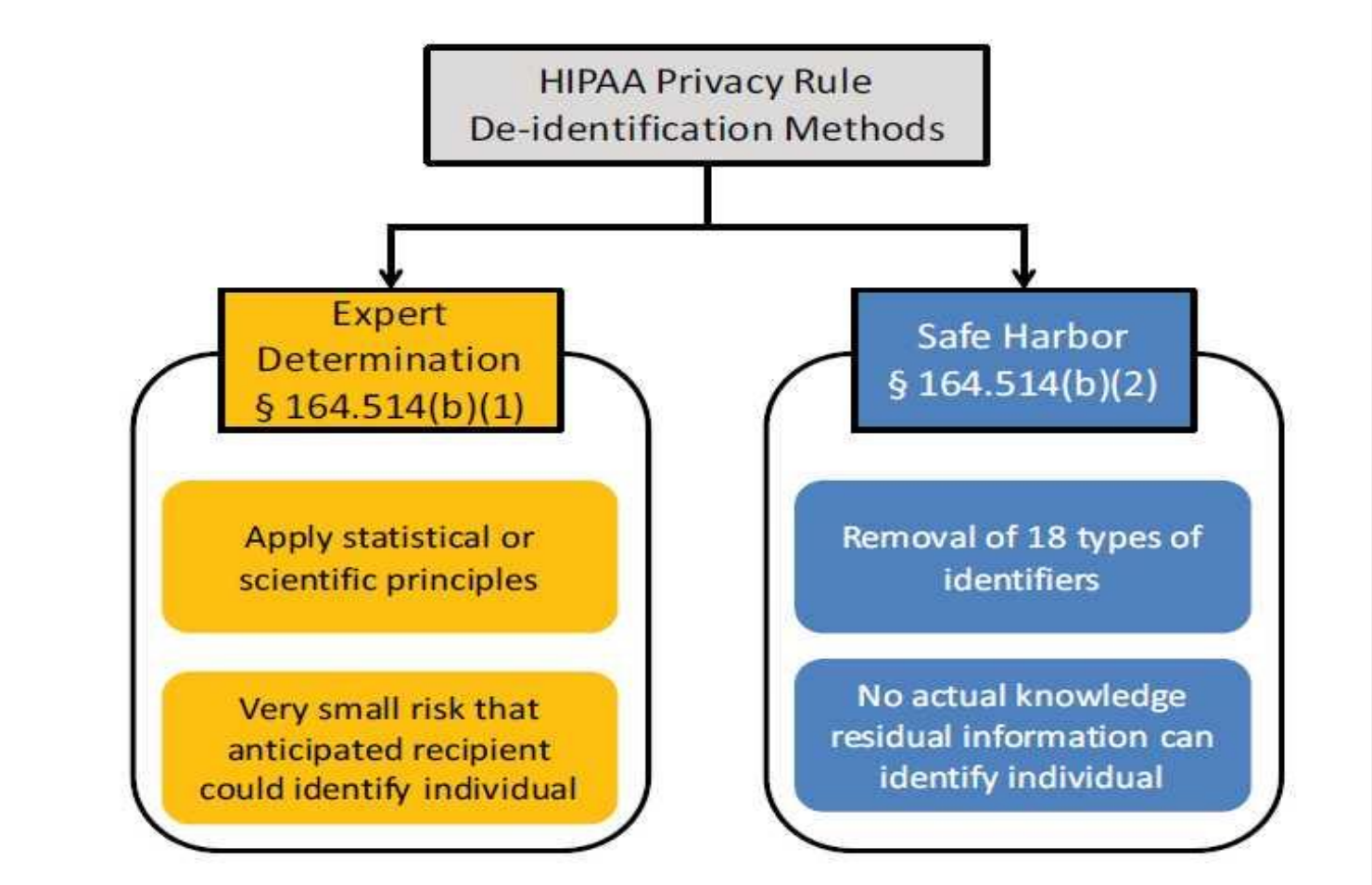
House Committee on Commerce and Economic Development

April 28, 2026

Vermont Data Privacy and Online Surveillance Act, S. 71 Draft No. 2.3

- My comments and viewpoints are solely my own
- My remarks will be confined to matters related to data de-identification and pseudonymization:
  - De-identification under HIPAA
  - De-identification under state privacy laws
  - Harmonization of de-identification standards under state privacy laws
  - Pseudonymization
  - Banning the re-identification of de-identified data

Two Methods of HIPAA De-identification



Source: HHS Office for Civil Rights (OCR) De-Identification Guidance (November 2012)

HIPAA Safe Harbor Method

All of the following must be removed for data to be de-identified under the Safe Harbor method:

(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 in §164.514(c)

45 CFR §164.514(b)(2)-(c)

HIPAA Expert Determination Method

Health Information is not individually identifiable if:

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;

45 CFR §164.514(b)

De-Identification under State Privacy Laws

Most state laws have two tiers of de-identification –

1) **For medical data, they harmonize with the HIPAA de-identification standard**
2) **For consumer and all other data, they apply their own state-specific de-identification standard**

CONNECTICUT (C.G.S.A. § 42-515)

"Deidentified 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 (A) takes reasonable measures to ensure that such data cannot be associated with an individual, (B) publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data, and (C) contractually obligates any recipients of such data to satisfy the criteria set forth in subparagraphs (A) and (B) of this subdivision.

IOWA (Iowa Code § 715D.1)

"De-identified data" means data that cannot reasonably be linked to an identified or identifiable natural person.

Harmonization of De-Identification Standards

- HIPAA de-identification standard has been foundational for more than 20 years
- CA's ground-breaking privacy law, the CCPA, initially didn't recognize HIPAA de-identification, using its own state-specific definition. Raised concerns. The CA legislature amended the CCPA in 2020 to harmonize with HIPAA de-identification for medical data
- CA testimony from the Association of Clinical Research Organizations: "*De-identification of individually identifiable health information is the single most effective method for protecting the confidentiality of health data, while facilitating its use for research.*"
- Disparate, state-specific de-identification standards and definitions add complexity, delays, confusion, contracting problems, and legal costs. Without advancing privacy. Harmonization is key.

Pseudonymization

- European law concept. Now appearing in some U.S. state privacy laws, including VT S. 71
- Pseudonymized data has had direct and indirect identifiers removed but not destroyed, and the linkage to identifiers is kept separately and securely.
- Pseudonymized data is not de-identified. It’s still subject to privacy laws.
- Pseudonymization is seen as a valuable privacy and security safeguard. Some state laws confer favorable treatment on its use. Some also require organizations that disclose pseudonymized data to exercise oversight over recipients.

Ban on Re-Identification of De-Identified Data

- In 2020, CA made it illegal to re-identify data that had been de-identified in accordance with HIPAA [essentially, de-identified medical and research data]
- Exceptions apply - specified medical, research, and public health purposes; for testing and validation; if required by law.
- Any re-identified data (even if re-identification was allowed) becomes subject again to applicable privacy laws

CA Civil Code sec. 1798.148(a)-(b)

Thank you for the opportunity to testify today.

Questions?

Reference Slides

De-Identification Definition in VT S. 71 Draft No 2.3

§2415a (19) “Deidentified data” means data that does not identify and cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to the individual, if the controller that possesses the data:

(A)(i) takes reasonable measures to ensure that the data cannot be used to reidentify an identified or identifiable individual or be associated with an individual or device that identifies or is linked or reasonably linkable to an individual or household; and

(ii) for purposes of this subdivision (A), “reasonable measures” includes the deidentification requirements set forth under 45 C.F.R § 164.514 (other requirements relating to uses and disclosures of protected health 8 information);

(B) publicly commits to process the data only in a deidentified fashion and not attempt to reidentify the data; and

(C) contractually obligates any recipients of the data to comply with all provisions of this subchapter.