CCPA and Other Potential State Laws – New Burdens on Medical Research and De-Identified Data

Ann Waldo, Waldo Law Offices
Dan Barth-Jones, Columbia University
Fielding Greaves, AdvaMed

October 16, 2019
Privacy & Security Forum

WLO
WALDO LAW OFFICES PLLC

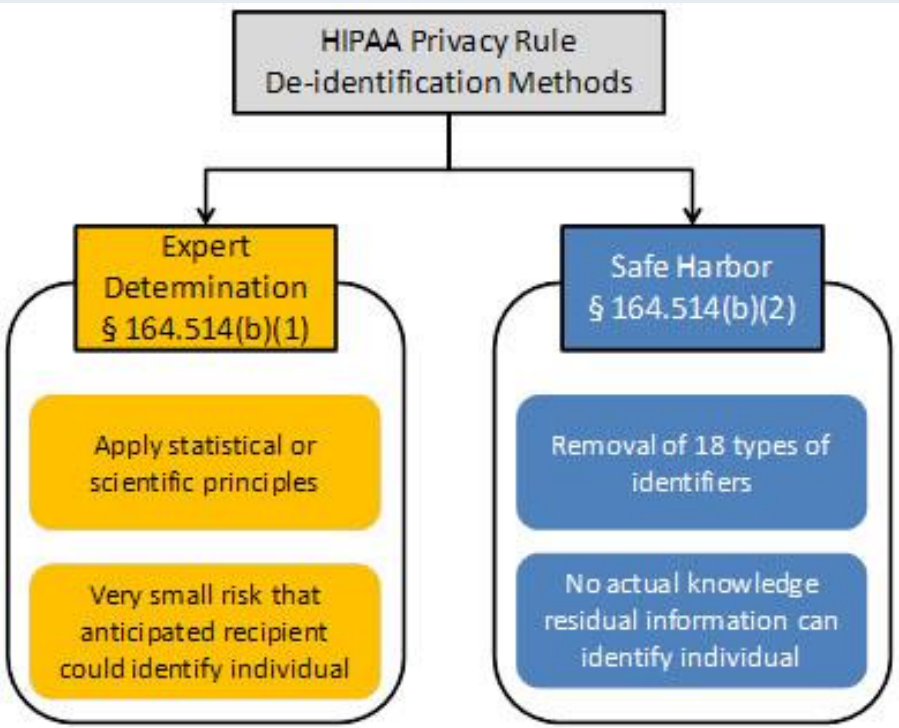
De-Identification and State Legislation

- **Status quo: HIPAA de-identification standard for health data**
- **State Legislation and de-identification:**
  - **What has already happened?**
  - **What almost happened in CA?**
  - **What might happen next?**
  - **What damage will these laws do to medical research?**

WLO
WALDO LAW OFFICES PLLC

De-Identification – Two Methods

HIPAA allows **two (and only two)** methods of de-identification, the Expert Determination and the Safe Harbor method.



WLO
WALDO LAW OFFICES PLLC

De-Identification - Safe Harbor Method

Safe Harbor method involves removing the following 18 identifiers of the individual or of relatives, employers, or household members of the individual:

1. Names;
2. 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.
3. 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;
4. Telephone numbers;
5. Fax numbers;
6. Email addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code, except as permitted by the re-identification rules, below; and

- The CE must 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.

De-Identification - Expert Method

Expert determination method involves:

- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
  a) 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
  b) Documents the methods and results of the analysis that justify such determination

What about re-identification risks under HIPAA?

Privacy Professionals note –

The highly publicized news stories about re-identification of de-ID'd health data did NOT involve data that was de-ID'd under the HIPAA standard!

Most of the reports about re-identification of de-identified data involve **hospital discharge data sets**, which are released under public health exception and are NOT subjected to HIPAA de-ID'n process. *The data is far too identifiable to qualify as HIPAA de-ID'd.*

WLO
WALDO LAW OFFICES PLLC

What has already happened?

- ❑ CCPA
- ❑ Nevada

WLO
WALDO LAW OFFICES PLLC

CCPA def. of “deidentified”

Current CCPA:

“Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2) Has implemented business processes that specifically prohibit reidentification of the information.
3) Has implemented business processes to prevent inadvertent release of deidentified information.
4) Makes no attempt to reidentify the information.

CA Civ Code 1798.140(h)

WLO
WALDO LAW OFFICES PLLC

3) De-identification under CCPA

- Problems for medical data and research -
  - CCPA definition of de-ID'n has no recognition of or exception for HIPAA de-ID'n standard
  - CCPA definition has four provisos related to business processes and conduct, not statistical standards.
    - These four provisos aren't impossible, but they are different from HIPAA.
- Interpretation is unclear and subject to dispute
- Anticipate disruption, delays, and expensive legal wrangling involving de-ID'd data

WLO
WALDO LAW OFFICES PLLC

Nevada

- Limited Do-Not-Sell rights
- Doesn’t affect de-identification; “covered information” is much narrower than Personal Information under CCPA
- Clear carve-out for entities regulated by HIPAA

What almost happened in CA?

- ❑ AB 873
- ❑ Set of healthcare amendments

WLO
WALDO LAW OFFICES PLLC

What almost happened in CA?

1) AB 873
   - Passed Assembly; died in Senate Finance
   - Would have replaced CCPA deidentification definition with a standard based on 2012 FTC Staff Report:

> (h) "Deidentified" means information that does not identify and is not reasonably linkable, directly or indirectly, to a particular consumer, provided that the business makes no attempt to reidentify the information, and takes reasonable technical and administrative measures designed to:
> (1) Ensure that the data is deidentified.
> (2) Publicly commit to maintain and use the data in a deidentified form.
> (3) Contractually prohibit recipients of the data from trying to reidentify the data.

   - NOTE – still no recognition of HIPAA de-ID'n standard. Thus could still anticipate legal confusion and wrangling

What else almost happened?

2) A set of medical research and healthcare amendments

- To have CCPA recognize HIPAA de-ID'n standard for data that was previously PHI (or identifiable medical research data)
- To expand clinical research data exemption
- To slightly broaden exemption for HIPAA business associates

- Eventually won support of privacy advocates
- Key support from AdvaMed
- Nonetheless, Sen. Judiciary Chair declined to advance them
- Door is open to re-introduce them in January

What might happen next?

Selected bills:

- ❑ New Jersey
- ❑ New York
- ❑ Oregon
- ❑ Washington

❑ CCPA 2.0

WLO
WALDO LAW OFFICES PLLC

Pending and/or Future Legislation

New Jersey A4640

- Similar de-ID'n language as in CCPA
- No HIPAA de-ID'n recognition
- PII language differs:

> "Personally identifiable information" means any information that personally identifies, describes, or is able to be associated with a data subject, including, but not limited to:
> . . .

WLO
WALDO LAW OFFICES PLLC

Pending and/or Future Legislation

NY A 8526

- Divergent definition of de-identification. No HIPAA recognition

"De-identified data" means:
(a) data that cannot be linked to a known natural person without additional information not available to the controller; or
(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

Pending and/or Future Legislation

OR 703 (failed)

- Introduced in multiple states
- A twist – definitions (including de-ID'n) are consistent with HIPAA
- But - **gives patients a PROPERTY interest in their health data, including de-ID'd data**
- Illegal to disclose health information or de-ID'd data unless the patient signs authorization saying she can elect to get a share of remuneration received by anyone for the disclosure of her data
- No exception for research, studies of quality or comparative effectiveness of treatments, etc.
- Drew fire from HC entities and privacy groups
- Proponent is a block chain company whose motto is "*Everyone has the right to legal ownership of their inherent human data as property*"

WA

WA SB 5376 (failed)

- Closer to GDPR than CCPA
- De-ID'n definition diverges from HIPAA's and doesn't recognize the HIPAA standard for health data
- Business support; will return in 2020

> "Deidentified data" means:
> (a) Data that cannot be linked to a known natural person without additional information kept separately; or
> (b) (b) Data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls.

WLO
WALDO LAW OFFICES PLLC

CCPA 2.0 (Ballot Initiative)

CA Privacy Rights and Enforcement Act of 2020

- Yet another definition of de-ID'n. No recognition of HIPAA de-ID'n standard

(k) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable consumer, provided that the business that possesses the information:
(A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;
(B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except as necessary to ensure compliance with this subdivision; and
(C) contractually obligates any recipients of the information to comply with al provisions of this subdivision.

WLO
WALDO LAW OFFICES PLLC

Importance of De-Identified Medical Data

Vast beneficial current and future uses of de-ID'd medical data and AI

- *De-ID'd data and sophisticated analytics improve research, innovation, cost reduction, regulatory compliance, care delivery, resource allocation, fraud detection – and cures for individuals*
- A top priority of the bipartisan 21st Century Cures Act
- De-ID'd data helps determine unmet medical needs, fight opioid crisis, identify sub-par care
- Consumer decision tools to understand benchmarked costs and outcomes through transparency
- UCSF Center for Intelligent Imaging accelerating research on advanced imaging using AI for diagnosis
- **Oncologists use de-ID'd data and advanced AI analytics to identify tumor mutations and map them to evidence-based therapies**

WLO
WALDO LAW OFFICES PLLC

Importance of De-Identified Medical Data

Vast beneficial current and future uses of de-ID'd medical data and AI

- Supports massive government policy shift from fee-for-services care toward payment for value/outcomes
- Benchmarked data gives providers crucial info about comparative medical outcomes, safety, and costs
- "Synthetic medical data" can be created based on actual de-ID'd data that speeds research and reduces costs
- FDA Commissioner: "Leveraging Real World Evidence is 'Top Programmatic Priority' for FDA"
  - RWE accelerates research, monitors drug and device safety, supports clinical decision-making, informs clinical guidelines
  - Google "FDA real world evidence" to learn more!

WLO
WALDO LAW OFFICES PLLC

What damage will divergent de-ID'n standards due to medical research and HC?

- Extent of damage - unknown and unknowable
- Uncertainty
- Legal disputes and expenses
- Business friction and delays
- Mounting cost of new drugs and devices
- Contractual wrangling

What do you think?

What should be done in terms of advocacy?

WLO
WALDO LAW OFFICES PLLC