Beyond HIPAA: US State Impact on Privacy Compliance

Presented by: **Greg Leighton**, Partner, Chicago Office
Meghan O'Connor, Partner, Milwaukee Office

April 22, 2022
HIPAA Collaborative of Wisconsin

Quarles & Brady LLP

1

Speakers

Greg Leighton
gregory.leighton@quarles.com
(312) 715-5094

Meghan O'Connor
meghan.oconnor@quarles.com
(414) 277-5423

2

Welcome and Agenda

CURRENT STATE:
BASICS OF A PRIVACY PROGRAM

ACT NOW:
NEW US STATE PRIVACY LAWS

FUTURE STATE:
WHAT'S NEXT?

3

Current State: Basics of a Privacy Program

Quarles & Brady LLP

4

US Privacy Basics

- Sectarian System – patchwork of laws focused on certain data or data subject types (e.g. HIPAA)
- Comprehensive Laws – newer but growing in prominence
- US Health Care organizations now need to worry about both!
- Developing US privacy laws are becoming nationwide best practice, even for health care entities

Quarles & Brady LLP 5

5

Privacy Policy

- From website to all data collection
- Core Content
  - Types of personal information collected
  - How and when personal information is collected
  - Purpose for collecting the personal information
  - Types of personal information "sold"
  - Third parties to which personal information is disclosed
  - Description of consumer rights
  - Contact information for questions or requests
- At least annual review and whenever there is a significant change in data collection or use practices or new legal requirements

Quarles & Brady LLP 6

6

Terms of Use

- Privacy Policy is a notice, while the Terms of Use is an agreement between the company and end-user
- Content Requirements:
  - Acceptance of terms
  - License to use
  - Acceptable use policy
  - Company's rights and ownership
  - International use and compliance
  - User accounts
  - Modification of site
  - Privacy notice reference
  - Disclaimers
  - Termination and modification

Quarles & Brady LLC 7

7

Data Mapping

- Identify key players within the organization with knowledge on data collection, use, and storage
- Conduct interviews and/or send questionnaires for details
- Assess and compile information in a data map
- Follow up with outstanding questions or gaps in data map
- Maintain the data map
- Makes risk analyses much easier

Quarles & Brady LLC 8

8

Data Retention and Destruction

- You can no longer keep data forever
  - Data minimization (CA, CO, VA)
  - Data retention must be a reasonable time period
  - Disclose retention period at time of collection (CA)
- Leverage your data map – what do you have and why?
- Destroy data securely
- Do not forget about email
  - Legal holds
  - Business email compromises are common

Quarles & Brady LLC 9

9

Data Retention

- Considerations:
  - Time needed to provide services (not all data is PHI)
  - Legal retention requirements
  - Statute of limitations/time necessary for protection from prosecution
  - Data management costs
- Data Minimization
  - EU: Only collect and maintain personal data for purposes that are adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed
  - CO and VA: Limit collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed
  - CA: Limit data collection and maintenance to what is necessary for the purpose the data is collected. Inform consumers about retention time for each category of personal information collected or criteria used to determine retention

10

Data Security is Part of Privacy

- Incident response
  - Tabletop – practice!
  - Support partners engaged in advance. Take advantage of A-C privilege
  - Don't forget about business continuity / disaster recovery plans as well
  - You have more than PHI
- Risk analysis
  - Annual cybersecurity audits if processing presents significant risk to consumer privacy / security (CA)
  - Should inform safeguards
  - Looks a lot like the HIPAA risk analysis
- Safeguards (CA, CO, VA)
  - *Establish, implement, and maintain* reasonable *administrative, physical, and technical* safeguards to protect *confidentiality, integrity, and accessibility* of personal data
  - Should be appropriate to risk and volume, nature, and scope of personal data / processing at issue
  - Looks a lot like HIPAA, but watch for guidance on technical specifics

11

Vendor Contracting

- Determine what vendors you have that touch personal data
  - *e.g.,* SaaS platform, payment processing, website hosting
- Review contracts to make sure they contain adequate privacy and security provisions that can evolve
- Negotiate and execute any necessary data processing agreements and contract addenda
  - Data processing agreements (GDPR)
  - Service provider addenda (CA)
  - Business associate agreement (HIPAA)

12

Act Now:
New US State Privacy Laws

Quarles & Brady LLP

13

State Privacy Laws Overview

- CCPA
- CPRA Amendments to CCPA
- Virginia
- Colorado
- Utah

Quarles & Brady LLP 14

14

HIPAA Carve-Outs

- Carve out based on entity vs. data
- De-identified data
  - CCPA does not apply to de-identified data originating from PHI if:
    - De-identified pursuant to HIPAA
    - Data not re-identified (with limited exceptions)
  - Website privacy policy must provide notice re: sale/licensing of de-identified data originating from PHI
  - Contract with recipient must include specific requirements and prohibitions

Quarles & Brady LLP 15

15

CPRA Basics

- Effective Jan. 1, 2023 with a data "look-back" until Jan. 1, 2022
- Applies to companies doing business in California that meet one of the following:

1. $25M Annual Revenue
2. Data from 100,000 CA consumers
3. Generate at least 50% of revenue through selling *or sharing* data

Quarles & Brady LLP 16

16

CPRA Scope

- All CA Personal Information not subject to an exemption
- Standard CCPA exemptions still apply:
  - Health Data subject to HIPAA/CMIA
  - Data subject to FCRA or GLBA
  - Vehicle/DL data, etc.
- Existing exemptions for employee data and so-called "B2B" data expire Jan. 1, 2023
- Beware further legislation on this point in 2022!

Quarles & Brady LLP 17

17

New Key Definition

- Sensitive Personal Information
  - SSN, DL, Passport, or other governmental ID
  - Account login & password including account numbers or usernames
  - Precise geolocation
  - Race, ethnicity, religious beliefs, union membership
  - Contents of consumers' mail, email, texts unless directed at the business
  - Biometrics, genetics, health, sex life or orientation
- Substantially broader than "Special Categories" under GDPR
- Health information that is not PHI is sensitive personal information

Quarles & Brady LLP 18

18

Consumer Rights – CCPA Rights in Place Now

- All CCPA rights still exist
- Access
- Deletion
- Non-discrimination
  - Likely to take on heightened importance in light of new rights to be exercised
  - But financial incentive to retain data (with notice) still appears to be permitted
- Authentication still required
- Methods of exercise under CCPA remain intact but companies will be incentivized to eventually allow opt-out through technical means

Quarles & Brady LLP 19

19

Consumer Rights – What's New Under CPRA?

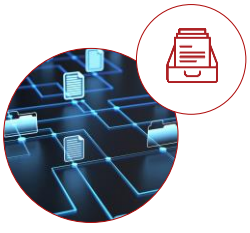
- Correction
- Opt-out of Sharing (or selling)
- Restrict Use of Sensitive PI
- Access information regarding Automated Decision-Making (or profiling)
  - Work Performance
  - Economic situation
  - Health
  - Personal Preferences/Interests
  - Reliability or behavior
  - Location or movements
- Opt-Out of Automated Decision-Making
- Opt-Out of Cross-Context Behavioral Advertising

Quarles & Brady LLP 20

20

CPRA Operational Requirements

- Data Minimization
- Published Retention Schedules
- Augmented data processing agreements
- Risk Assessments and Audits for "High-Risk" Processing



Quarles & Brady LLP 21

21

Data Minimization & Retention

- Collection, use, retention, and sharing must be reasonably necessary and proportionate to achieve the purpose of collection or processing or another disclosed purpose compatible within the context of collection.
  - Feels like HIPAA's minimum necessary standard
- Disclosure of retention periods required
  - At time of collection
  - Each category of PI collected
  - May not be longer than reasonably necessary for each disclosed purpose

Quarles & Brady LLP 22

22

Processing Agreements

- Contracts between businesses and Service Providers, Contractors, & Third-Parties required
  - Processing limitation
  - Required CPRA compliance of processor and subprocessors
  - Compliance Monitoring
  - Notification of non-compliance
  - Cooperation with data subject requests
- Much closer to Art. 28 of GDPR
- More than a BAA

Quarles & Brady LLP 23

23

Risk Assessments

- Standard – "significant risk to consumers' privacy or security" (CPPA to further define in implementing regulations)
- Annual audits and reports submitted to CPPA
- Assessments for high-risk processing activities to be documented
  - Benefits of processing
  - Risks to Consumers
- Size and complexity of the business should be taken into account

Quarles & Brady LLP 24

24

CPRA – Children's Data

- Children = under 16 years old
- Triple fines for violations
- Affirmative opt-in required to sell or share data
- 1 year waiting period for repeating an opt-in request
- Be careful with marketing programs. This is more than a HIPAA marketing authorization

Quarles & Brady LLP 25

25

CPRA – Expanded Breach Liability

- Definition of data breach expanded to include unauthorized access or disclosure of an email address and password or security question that would permit access to an account if the business failed to maintain reasonable security.
- Subject to the Private Right of Action
- All other CCPA security and breach provisions remain in-force
- HIPAA breach notification remains in-force

Quarles & Brady LLP 26

26

Enforcement

- All enforcement and rulemaking now vested in CPPA
- Agency will self-fund through fines
- Removal of 30-day cure period
- Enforcement frequency likely to increase significantly in 2023

Quarles & Brady LLP 27

27

CPRA Compliance Checklist

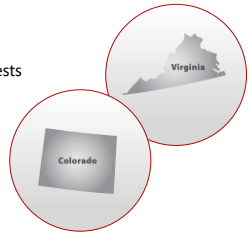
- Evaluate potential operational impacts of new opt-outs or opt-in requirements
- Update Privacy Policy with relevant retention periods
- Amend vendor agreements as necessary
- Expand data subject response program to accommodate new rights
- Ensure no discriminatory actions for exercise of rights
- Develop process for privacy audit and assessments of new products, initiatives, and vendors

Quarles & Brady LLP 28

28

Don't Forget Colorado, Virginia, & Utah

- Very similar to CPRA
- Additional requirements:
  - Appeals process for data subject requests
  - Universal tech opt-out by 2024
  - Data Portability
- Don't forget state laws re:
  - Biometric data
  - Genetic data



Quarles & Brady LLP 29

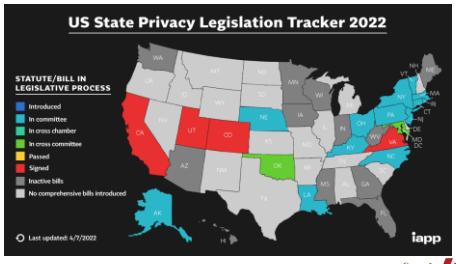
29

Future State: What's Next?

Quarles & Brady LLP

30

A Look Ahead in 2022



Quarles & Brady LLC 31

31

Future State Components

- PIA / DPIAs
- Remote work data collection / access
- Biometrics / facial recognition
- Long-term guesses

Quarles & Brady LLC 32

32

Privacy Impact Assessments

- Currently required under limited circumstance
- Soon will be broadly required for most processing activities
- Key takeaways:
  - Develop internal reporting structures with business teams
  - Establish a repeatable and scalable assessment and documentation process
  - Secure necessary resources
  - Can be part of your HIPAA risk analysis process, but it will expand to Personal Information not just PHI

Quarles & Brady LLC 33

33

Remote Work

- Health/vaccination data
- Data breach risks resulting from remote work
- Additional collection of remote employee data

34

Biometrics / Facial Recognition

- Comprehensive laws will be a floor but watch out for specific laws or pieces of laws regarding these topics
- Three states already have biometrics laws with more on the way
- Many states are considering specific regulations on facial recognition
- Extra compliance:
  - Special notices
  - Heightened security
  - Data segmentation/use limitation

35

Guesses for the Future

- European-style cookie banners are likely to be required in the US and most countries around the world
- Future legislation is likely to regulate AdTech in specific ways not yet seen
- CPO likely to become a required role for more organizations
- Limited private right of action to enforce privacy rights likely to emerge eventually in the US
- More challenging M&A without proper individual authorization

36

Privacy Program Checklist

- Identify applicable privacy laws / regulations
- Establish internal privacy team / reporting structure
- Data Map and Risk Analysis
- Ensure that all major policies are in place
  - Website Privacy Notice / Terms
  - Information Security
  - Incident Response
  - Business Continuity / Disaster Response
  - Data Retention / Destruction
  - Employee Privacy Policy

37

Privacy Program Checklist

- Develop schedule for regular audits and revision of policies
- Establish regular and updated privacy training program
- Implement major processes
  - Destruction and remediation of legacy data sets
  - Vendor diligence / contractual compliance
  - Response to data subject requests
  - PIAs

38

Thank You. Questions?

Greg Leighton
gregory.leighton@quarles.com
(312) 715-5094

Meghan O'Connor
meghan.oconnor@quarles.com
(414) 277-5423

39