Navigating the Digital Health Legal Landscape: User Guide to State Data Privacy Laws

AzSHA
Arizona Society of Healthcare Attorneys

JAMES E. ROGERS COLLEGE OF LAW
Health Law

TechLaw

ARIZONA TELEMEDICINE PROGRAM

SOUTHWEST TRC TELEHEALTH RESOURCE · CENTER

Land Acknowledgement

We respectfully acknowledge the University of Arizona is on the land and territories of Indigenous peoples. Today, Arizona is home to 22 federally recognized tribes, with Tucson being home to the O'odham and the Yaqui. The Southwest Telehealth Resource Center represents CO, AZ, NM, NV and the Four Corners Region with a combined total of 72 recognized tribes. The university strives to build sustainable relationships with sovereign Native Nations and Indigenous communities through education offerings, partnerships, and community service.

Webinar Tips & Notes

- When you joined the webinar your phone &/or computer microphone was muted
- Time is reserved at the end for Q&A, please use the **Chat function** to ask questions
- Please fill out the post-webinar evaluation
- Webinar is being recorded
- Recordings will be posted on the ATP website
    - http://telemedicine.arizona.edu/webinars/previous

Navigating the Digital Health Legal Landscape: User Guide to State Data Privacy Laws

Tara Sklar, JD, MPH

Associate Director of Telehealth Law & Policy

Arizona Telemedicine Program

Faculty Director of the Health Law & Policy Program

Distinguished Public Service Scholar

University of Arizona James E. Rogers College of Law

Certificate Information, CLE Credit

The State Bar of Arizona does not approve or accredit CLE activities for the Mandatory Continuing Legal Education (CLE) requirement. This activity may qualify for up to 1 hour of CLE credit toward your annual requirement for the State Bar of Arizona.

CLE Certificates of Attendance can be requested within the evaluation following this webinar. Melanie Escher will be sending a thank you email with directions and the evaluation link. Certificates will be sent by Melanie to individual emails as requested.

Panelists

John F. Howard
Senior Attorney
Clark Hill PLC

Chase Millea
Attorney
KO Law PC

Claudia E. Stedman
Attorney
Snell & Wilmer, LLP

Topics

- HIPAA key developments affecting digital health operations.
- Trends in state data privacy legislation.
- Practical strategies for enhancing data privacy and staying abreast of the changing legal landscape.

John F. Howard
Senior Attorney
Clark Hill PLC

Professor of Practice
University of Arizona
James E. Rogers College of Law

Health Insurance Portability and Accountability Act

Purpose & Scope

Create alignment between health care entities through established standards and allow for the portability of health information

Three Main Rules: Privacy Rule (2001); Security Rule (2005); Breach Notification Rule (2006)

Applicable Information:

1. Individually Identifiable Health Information (IIHI)
2. Protected Health Information (PHI)

Covered Entities: Health Care Providers; Health Care Clearing Houses; Health Plans

Health Insurance Portability and Accountability Act

State Law Preemption

General Rule: HIPAA standards, requirements, and implementation specifications preempt State law that is contrary or provides less protection, or is less stringent, than those provided under HIPAA.

Some exceptions provided:

1. Procedures that provide for reporting of disease/injury; child abuse, birth, or death; or public health surveillance activities
2. Certain auditing, monitoring, or reporting activities
3. To prevent fraud and abuse

Health Insurance Portability and Accountability Act

Notable Activity

1. Proposed Security Rule Updates

- Issued Dec. 27. 2024 – Comment Period Ends March 7, 2025

2. Reproductive Health Care Privacy Rule

- Currently being challenged by Texas AG in Federal Court

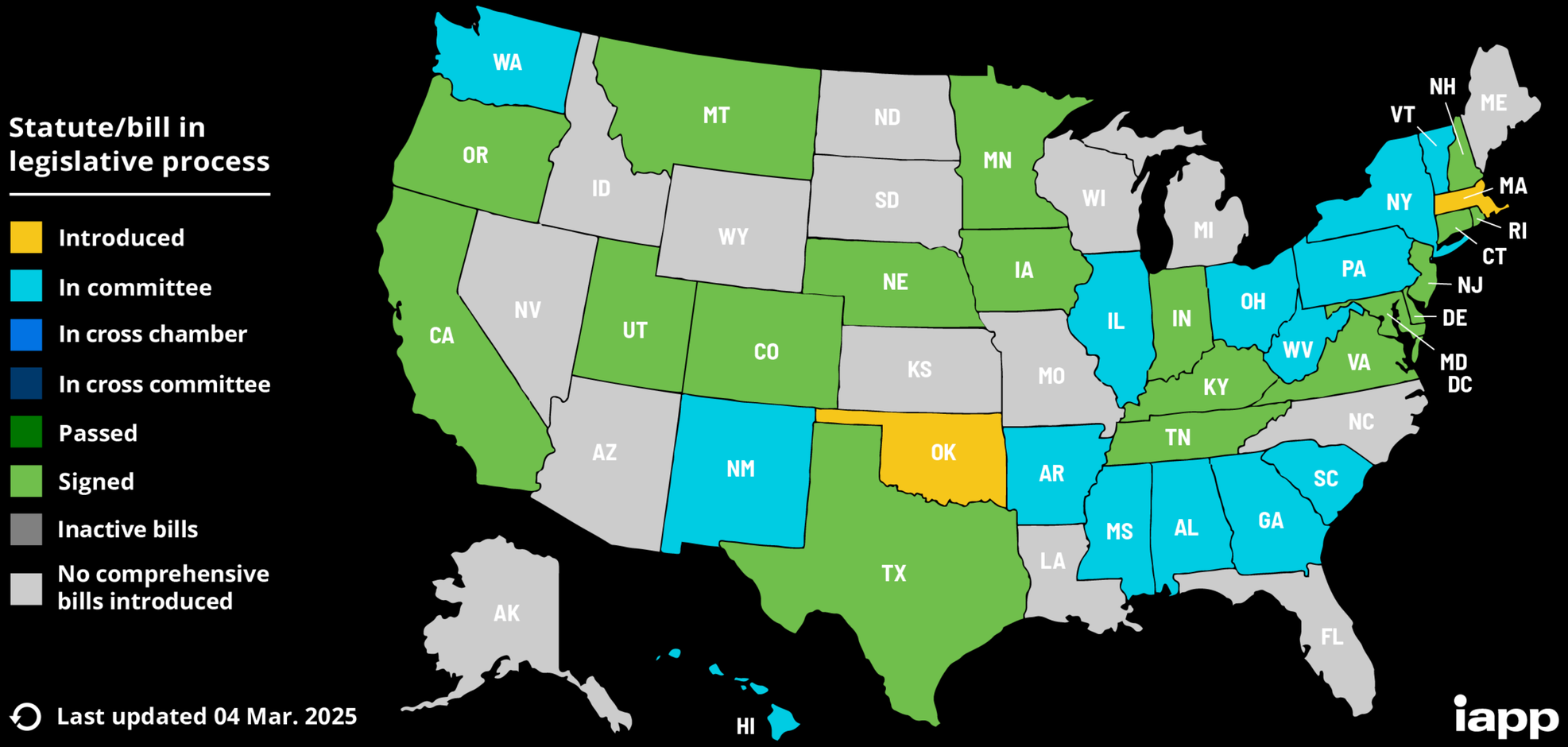
3. Website Tracking Technologies

- US District Court, Northern District of Texas order OCR vacate its guidance
- Involved online tracking technologies and IIHI

Chase Millea
Attorney
KO Law PC

Professor of Practice
University of Arizona
James E. Rogers College of Law

US State Privacy Legislation Tracker 2025



State Consumer Privacy Laws – Overview

State Consumer Privacy Laws – Basic Requirements

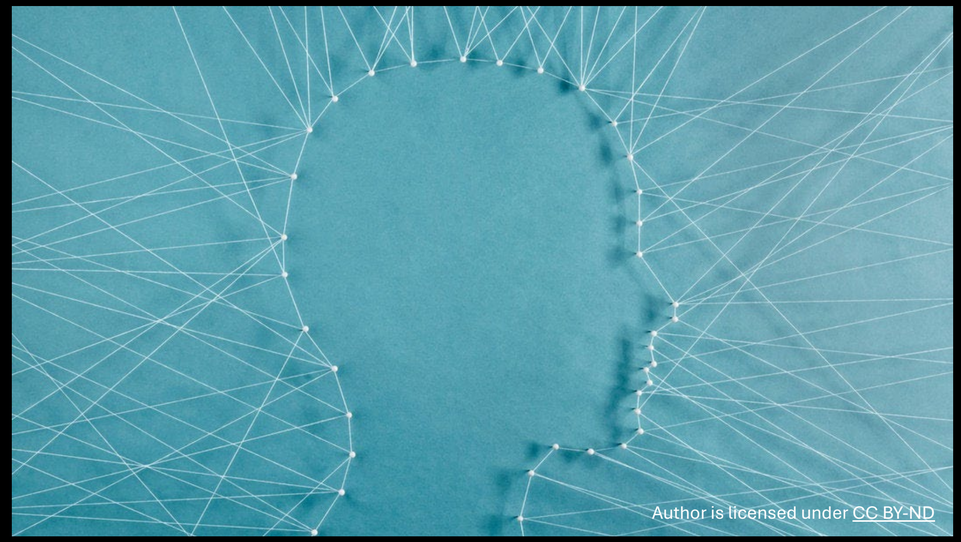
1. **Data Minimization**: *reasonably necessary and proportionate* to achieve purpose for which information was collected.
2. **Notice Requirements**:
   - Privacy Policy
   - Consent for sensitive data
   - Disclosures for sales/targeting advertising
3. **Consumer Rights (depending on State)**:
   - Know
   - Access & Portability
   - Correction
   - Deletion
   - Opt out of Sales/Sharing/Targeting Advertising
   - Limit Use of Sensitive Data
   - Non-Discrimination
4. **Security**
5. **Contractual Requirements**: *data processing agreements (DPAs)* with sub-processors

State Consumer Privacy Laws – Consumer Health Data

Recent laws in **Washington, Nevada, Connecticut** regulating "*consumer health data*"

Basic Requirements:
- Specific Notices
- Consent Requirements
- Consumer Rights
- Geofencing restrictions (around healthcare service providers)
- Private Right of Action (Washington)

Exceptions:
- Information maintained by HIPAA covered entity or business associate (Washington)
- Entity subject to HIPAA (Nevada)
- Protected Health Information (Connecticut)



Claudia E. Stedman
Attorney
Snell & Wilmer, LLP

Data Privacy & Security Implications for Telehealth

- ***What is telehealth?***
  - The use of digital information and communication technologies to access health care services remotely.
- ***How has telehealth affected healthcare delivery in the U.S.?***
  - During the COVID-19 pandemic, HHS and CMS waived a number of regulatory requirements so that providers could deploy virtual services to patients.
  - 54% of Americans have now had a telehealth visit – and satisfaction among telehealth users remains high.

Data Privacy & Security Implications for Telehealth

Risks to Patients' ePHI

- Cybersecurity threats
- Privacy concerns
- Regulatory changes

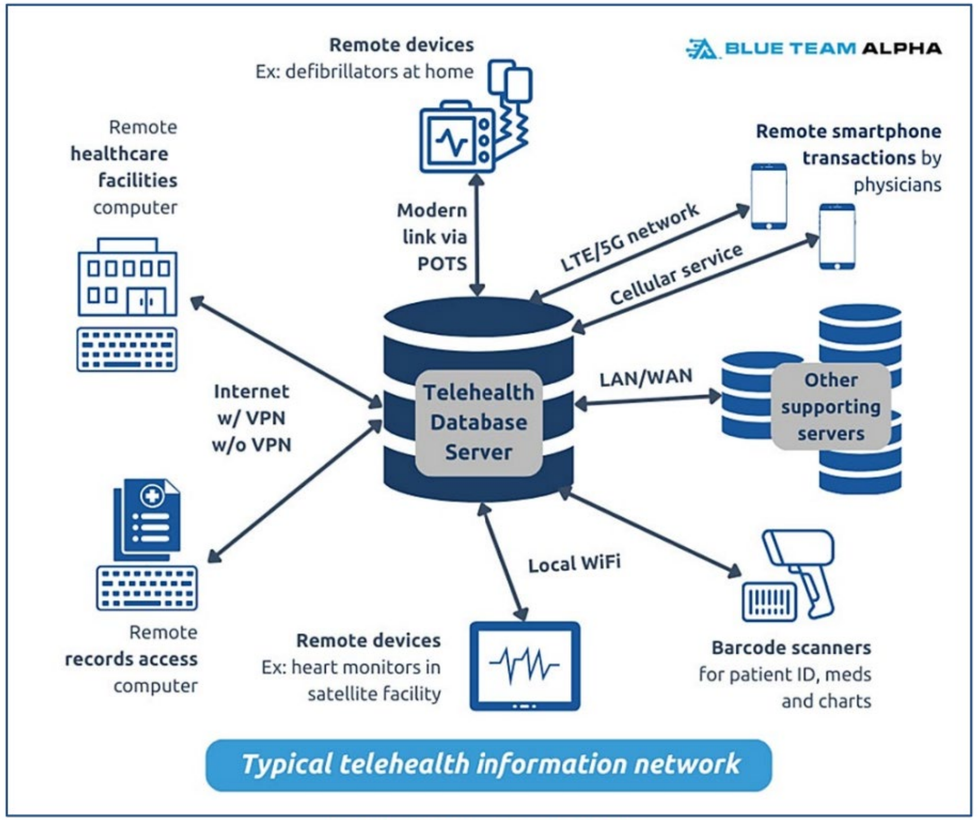
Best practices for securing patient data

- Patient and workforce education
- HIPAA-compliant telehealth platforms
- Regulatory compliance

SNELL & WILMER

Data Privacy & Security Implications for Telehealth

- HHS recently published guidance on cybersecurity for telehealth platforms reiterates software and practice compliance best practices for safeguarding PHI.
- Consider how information is recorded, stored, and, if using AI platforms, ensure that the patient has consented and consider whether that information becomes part of the designated record set.



Source: Blue Team Alpha

SNELL & WILMER

Navigating the Digital Health Legal Landscape: User Guide to State Data Privacy Laws

AzSHA
Arizona Society of Healthcare Attorneys

JAMES E. ROGERS COLLEGE OF LAW
Health Law

TechLaw

ARIZONA TELEMEDICINE PROGRAM

SOUTHWEST TRC TELEHEALTH RESOURCE · CENTER

Your opinion is valuable to us.
Please participate in this brief evaluation!

Evaluation link sent in thank you email to live event participants.

This webinar is made possible through funding provided by Health Resources and Services Administration, Office for the Advancement of Telehealth (U1U42527).