December 9, 2024

# Health Law Navigator: HIPAA and Privacy Update

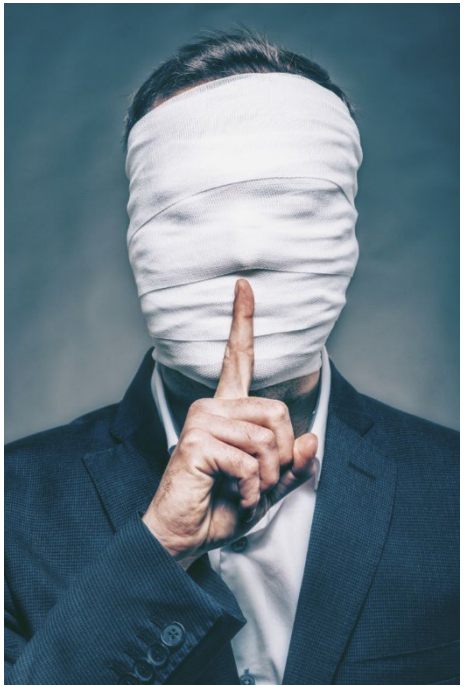
Stacy Harper
Christine Chasse

SpencerFane®

# Agenda

- Privacy Basics
- 42 CFR Part 2
  - Before
  - New Flexibility and Enforcement
- HIPAA
  - Before
  - Reproductive Health Records
- Notice of Privacy Practices
- Business Associate Agreements
- Other Privacy Changes
- Next Steps and Recommendations

# Privacy Basics



SpencerFane

# HIPAA

- Applies to Covered Entities and Business Associates
- Restricts the use and disclosure of Protected Health Information
- Imposes specific privacy, security and data breach notification requirements
- If state law is more restrictive, then state law prevails

# Protected Health Information (PHI)

- Individually identifiable health information that is transmitted in electronic media, maintained in electronic media, or transmitted or maintained in any other form, but not including education records covered by FERPA, certain higher education records, employment records held by a covered entity in its role as employer, and regarding a person who has been deceased more than 50 years.
- Health information means any information, including genetic information, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and relates to past, present, or future physical or mental health or condition of an individual, provision of health care, or past, present or future payment for the provision of health care.
- Individually identifiable means information that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual

# Business Associate

- A person/entity who, with respect to a covered entity:
  - On behalf of such covered entity or an organized health care arrangement, but other than as a member of the workforce of the covered entity, creates, receives maintains or transmits PHI for an activity regulated by HIPAA, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; patient safety activities; benefit management; practice management and repricing; or
  - Provides, other than as a member of the workforce, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the covered entity or organized health care arrangement where the performance of service involves the disclosure of PHI.
- BA includes a health information organization, e-prescribing gateway, or other person that provides data transmission services that requires access on a routine basis to such PHI; a person that offers a personal health record on behalf of a covered entity; and a subcontractor that receives, creates, maintains or transmits PHI on behalf of a BA.
- Certain exceptions

# 42 C.F.R. Part 2

- Applies to the Records created by Programs related to substance use diagnosis and treatment
- More restrictive than HIPAA
- Obligations stay with the information

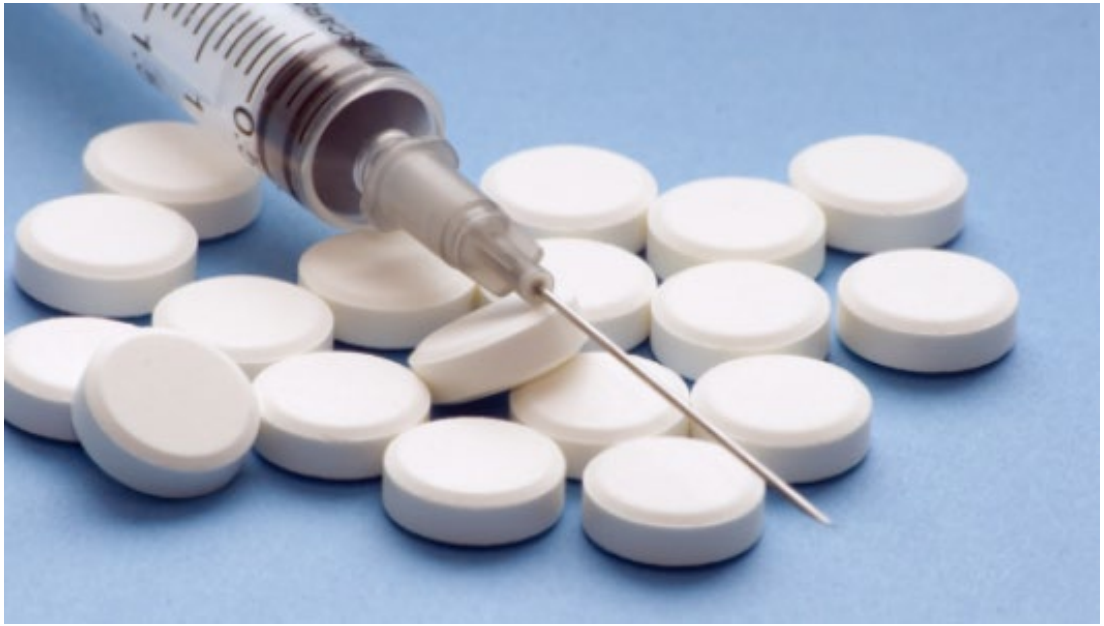
# Part 2 Program

- A person (other than a general medical facility) that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
- An identified unit within a general medical facility that holds itself out as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
- Medical personnel or other staff in a general medical facility whose primary function is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

# Part 2 Records

- Records means any information, whether recorded or not, created by, received, or acquired by a Part 2 program relating to a patient (e.g., diagnosis, treatment and referral for treatment information, billing information, emails, voice mails, and texts), and including patient identifying information, provided, however, that information conveyed orally by a Part 2 program to a provider who is not subject to this part for treatment purposes with the consent of the patient does not become a record subject to this part in the possession of the provider who is not subject to this part merely because that information is reduced to writing by that provider who is not subject to this part. Records otherwise transmitted by a Part 2 program to a provider who is not subject to this part retain their characteristic as records in the hands of the provider who is not subject to this part, but may be segregated by that provider.

# 42 C.F.R. Part 2



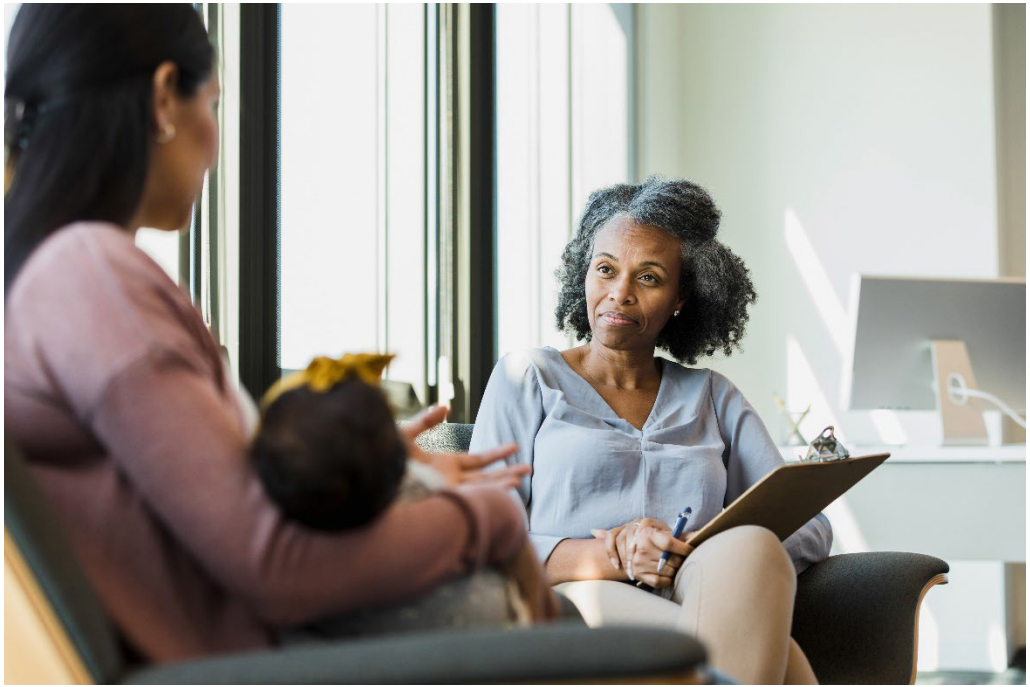
# Historic Part 2 Restrictions

- Requires authorization for almost all disclosures, including treatment, payment and health care operations
- Significant additional requirements for disclosure related to a court order, judicial proceeding, or law enforcement inquiry, distinguished by
  - Criminal investigation/prosecution of the patient
  - Non-criminal purposes
  - Investigation of the Part 2 Program
  - Referrals from the Criminal Justice System
  - Prescription Drug Monitoring Programs

# New Flexibility and Enforcement

- Allows single authorization for treatment, payment, and health care operations
- Allows recipient under that authorization may subsequently disclose the information for these purposes
- New definition and treatment of SUD Counseling Notes
- Each disclosure with consent must include copy of the consent or description of the scope
- Applies HIPAA breach notification requirements to Part 2 information
- Incorporates Part 2 into the HIPAA Notice of Privacy Practices
- Incorporates HIPAA penalties for enforcement

# HIPAA



SpencerFane

# HIPAA General Rules

- A covered entity or business associate may not use or disclose PHI except as permitted or required by HIPAA
- Authorization is required unless HIPAA allows disclosure without authorization

# HIPAA – Exceptions to Authorization

- Treatment, payment and health care operations
- Opportunity to object – individuals involved in care and facility directory
- Without authorization
  - Required by law
  - Judicial/administrative proceedings
  - Law enforcement
  - Health care oversight
  - Public health
  - Etc.

# HIPAA – Exception Considerations

- Recipient
- Purpose
- Scope
- Requirements

# Reproductive Health Care

- Reproductive health care means health care, as defined in this section, that affects the health of an individual in all matters relating to the reproductive system and to its functions and processes. This definition shall not be construed to set forth a standard of care for or regulate what constitutes clinically appropriate reproductive health care.
- Seeking, obtaining, providing, or facilitating reproductive health care includes, but is not limited to, any of the following: expressing interest in, using, performing, furnishing, paying for, disseminating information about, arranging, insuring, administering, authorizing, providing coverage for, approving, counseling about, assisting, or otherwise taking action to engage in reproductive health care; or attempting any of the same

# Prohibited Purposes

- A covered entity or business associate may not use or disclose protected health information for any of the following activities:
  - To conduct a criminal, civil, or administrative investigation into any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.
  - To impose criminal, civil, or administrative liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care.

# Prohibited Purposes: Applicability

- Rule of applicability. The prohibition applies only where the relevant activity is in connection with any person seeking, obtaining, providing, or facilitating reproductive health care, and the covered entity or business associate that received the request for protected health information has reasonably determined that one or more of the following conditions exists:
  - The reproductive health care is lawful under the law of the state in which such health care is provided under the circumstances in which it is provided.
  - The reproductive health care is protected, required, or authorized by Federal law, including the United States Constitution, under the circumstances in which such health care is provided, regardless of the state in which it is provided.
  - The presumption applies.
- Presumption. The reproductive health care provided by another person is presumed lawful unless the covered entity or business associate has any of the following:
  - Actual knowledge that the reproductive health care was not lawful under the circumstances in which it was provided.
  - Factual information supplied by the person requesting the use or disclosure of protected health information that demonstrates a substantial factual basis that the reproductive health care was not lawful under the specific circumstances in which it was provided.

# Prohibited Purposes, Cont'd

- In other words, this prohibition limits covered entities from using and disclosing PHI for the purpose of investigating or imposing liability related to reproductive health care that is legally provided under state or federal law, but it *does not* limit the use or disclosure of PHI related to reproductive health care that was not legally provided under state or federal law, although current HIPAA restrictions regarding use and disclosure of PHI continue to apply.
- In that case, a covered entity would be permitted, but not required, to disclose PHI to law enforcement if aligned with the Privacy Rule.

# Applicable Requests

- The attestation requirements apply to disclosures to
  - Health oversight activities;
  - Judicial and administrative proceedings;
  - Law enforcement; and
  - Coroners and medical examiners
- When the PHI is potentially related to reproductive health care

# What if You Cannot Separate Reproductive Health Care From the Rest of the Records?

- Reproductive health care is often inseparably intertwined with the patient's general medical records
- Consider if attestations should be completed with all PHI requests versus for only those potentially related to RHI.

# Attestation Requirements

- Effective December 23, 2024
- A description of the information requested that identifies the information in a specific fashion, including one of the following:
  - The name of any individual(s) whose protected health information is sought, if practicable.
  - If including the name(s) of any individual(s) whose protected health information is sought is not practicable, a description of the class of individuals whose protected health information is sought.
- The name or other specific identification of the person(s), or class of persons, who are requested to make the use or disclosure.
- The name or other specific identification of the person(s), or class of persons, to whom the covered entity is to make the requested use or disclosure.

# Attestation Requirements Cont'd

- A clear statement that the use or disclosure is not for a prohibited purpose.
- A statement that a person may be subject to criminal penalties pursuant to 42 U.S.C. 1320d–6 if that person knowingly and in violation of HIPAA obtains individually identifiable health information relating to an individual or discloses individually identifiable health information to another person.
- Signature of the person requesting the protected health information, which may be an electronic signature, and date. If the attestation is signed by a representative of the person requesting the information, a description of such representative's authority to act for the person must also be provided.
- Plain language requirement. The attestation must be written in plain language.
- If, during the course of using or disclosing protected health information in reasonable reliance on a facially valid attestation, a covered entity or business associate discovers information reasonably showing that any representation made in the attestation was materially false, leading to a use or disclosure for a prohibited purpose prohibited, the covered entity or business associate must cease such use or disclosure.

# Why was the Attestation Designed this Way?

- To put the burden on the requestor to establish that the information request is:
  - Needed
  - Permitted
  - Lawful

# Model Attestation

## Model Attestation Regarding a Requested Use or Disclosure of Protected Health Information Potentially Related to Reproductive Health Care

*The entire form must be completed for the attestation to be valid.*

| |
|---|
| Name of person(s) or specific identification of the class of persons to receive the requested PHI. |
| *e.g., name of investigator and/or agency making the request* |
| Name or other specific identification of the person or class of persons from whom you are requesting the use or disclosure. |
| *e.g., name of covered entity or business associate that maintains the PHI and/or name of their workforce member who handles requests for PHI* |
| Description of specific PHI requested, including name(s) of individual(s), if practicable, or a description of the class of individuals, whose protected health information you are requesting. |
| *e.g., visit summary for [name of individual] on [date]; list of individuals who obtained [name of prescription medication] between [date range]* |

I attest that the use or disclosure of PHI that I am requesting is not for a purpose prohibited by the HIPAA Privacy Rule at 45 CFR 164.502(a)(5)(iii) because of one of the following (check one box):

☐ The purpose of the use or disclosure of protected health information is **not** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care or to identify any person for such purposes.

☐ The purpose of the use or disclosure of protected health information **is** to investigate or impose liability on any person for the mere act of seeking, obtaining, providing, or facilitating reproductive health care, or to identify any person for such purposes, but the reproductive health care at issue was **not lawful** under the circumstances in which it was provided.

I understand that I may be subject to criminal penalties pursuant to 42 U.S.C. 1320d-6 if I knowingly and in violation of HIPAA obtain individually identifiable health information relating to an individual or disclose individually identifiable health information to another person.

*Signature of the person requesting the PHI*

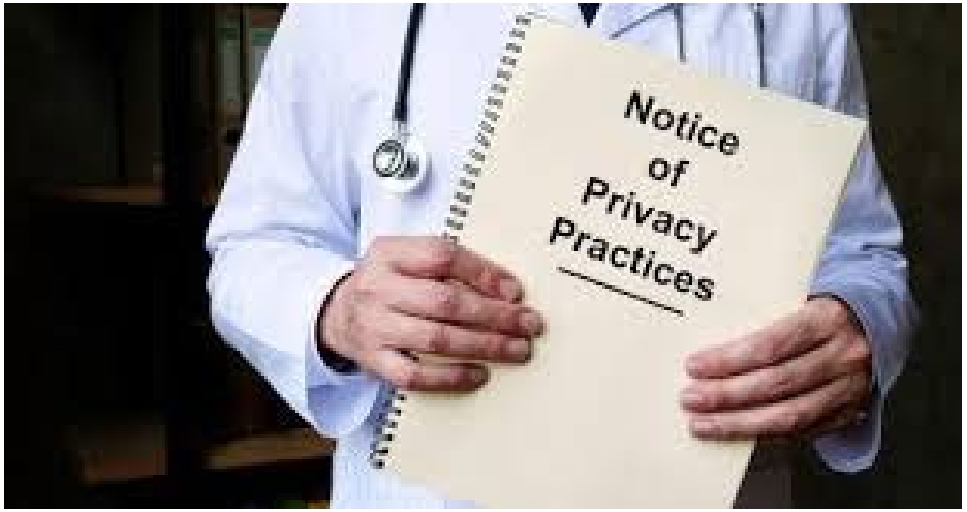
_____ Date _____

*If you have signed as a representative of the person requesting* PHI, *provide a description of your authority to act for that person.*

_____

SpencerFane

# Notice of Privacy Practices



# Notice of Privacy Practices (NPP)

NPPS need to be updated to include:

- Descriptions of the types of uses and disclosures of reproductive PHI prohibited under the Final Rule and an example of a prohibited use or disclosure;
- Description of the types and uses of disclosures of reproductive health PHI for which an attestation is required under the Final Rule, and an example of a use or disclosure for which an attestation is required; and
- Statement regarding the possibility that PHI disclosed to another person or entity may be redisclosed by that person or entity to other persons and entities.

# Notice of Privacy Practices, Cont'd

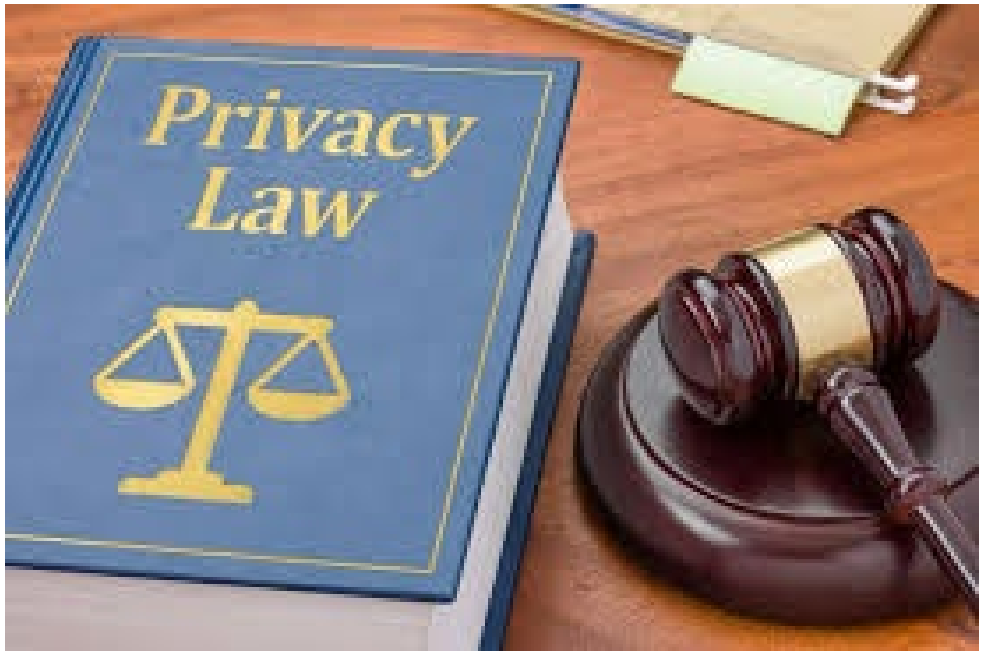
- Changes must be implemented by February 16, 2026
- Adds reference to applicability of records under Part 2
- If a law other than HIPAA (e.g. Part 2) restricts a disclosure, the more restrictive requirement must be described
- Must include description of attestation/reproductive rights requirements, including examples
- Notice that information disclosed may be subject to re-disclosure
- Notice of prohibition on use of Part 2 information for certain proceedings
- Ability to opt out of fundraising for Part 2 information

# Business Associate Agreements

# Business Associate Agreement

- Revisions automatically apply to business associates/recipients of Part 2 information
- Final rule expressly contemplated not requiring revision to all Business Associate Agreements
- Case-by-case analysis based on existing agreement language

# Other Privacy Changes



# New Laws

- Montana Consumer Data Privacy Act – Effective October 1, 2024
- Delaware Personal Data Privacy Act – Effective January 1, 2025
- Iowa Consumer Data Protection Act – Effective January 1, 2025
- Nebraska Data Privacy Act – Effective January 1, 2025
- New Hampshire Privacy Act – Effective January 1, 2025
- New Jersey Data Privacy Act – Effective January 15, 2025
- Tennessee Information Protection Act – Effective July 1, 2025
- Minnesota Consumer Data Privacy Act – Effective July 31, 2025
- Maryland Online Data Privacy Act – Effective October 1, 2025

# Common Themes

- Disclosing data practices to consumers
- Vendor agreement terms related to data processing/privacy
- Risk assessments
- Individual rights
  - Opt out
  - Deletion of data
  - Sensitive information considerations
- Timing: Usually entities only have a few months to develop and implement changes, as in our case study:

# Trend to Watch

- **Tracking Technologies**
  - A joint statement by HHS' OCR and FTC warned health care providers and app developers about the "serious privacy and security risks related to the use" of Tracking Technologies. Specifically, in certain circumstances, OCR interpreted the act of an individual visiting a website as evidence of a relationship or anticipated future relationship between the individual and the entity, making information related to that website visit PHI subject to HIPAA.
  - The FTC enforced the Personal Health Records Breach Rule in February 2023 against GoodRx Holdings, Inc. (GoodRx) related use of tracking technologies and alleged failure to notify consumers of its unauthorized disclosures of PHI.
  - Google and Meta, two of the largest providers of the Tracking Technologies, have also faced legal action related to their collection and use of health information.

# Potential New Trend: Case Study

- California's Assembly Bill No. 352 (AB 352)
- Effective January 1, 2024, and required by July 1, 2024
- Gender affirming care, abortion and abortion-related services and contraception
- Segregation requirements
- Restrictions on sharing information out of state
- Prohibition on disclosure for enforcement actions
- Exclusion from HIE

# Case Study AB 352, Con't:

- These requirements apply to a "business" that electronically stores or maintains medical information on the provision of sensitive services.
- A "business," as defined in Cal. Civil Code § 56.06, is ambiguous, and it includes, but is not limited to: businesses that maintain medical information for individuals or providers, offer software or hardware to manage medical information, or provide a digital service related to reproductive or sexual health.
- Whether this law applies to businesses located outside of California that serve California residents is unclear.

# Case Study AB 352, Con't:

- Health care providers, service plans, contractors, and employers are prohibited from cooperating with any inquiry or investigation by, or providing medical information to, an individual, agency, or department from another state or a federal law enforcement agency that would identify an individual seeking or obtaining an abortion or abortion-related services that are lawful under California law, *unless* the request for medical information is authorized under existing law provisions.
- Health care providers are exempt from liability for damages or from civil or enforcement actions relating to cooperating with, or providing medical information to, another state or a federal law enforcement agency before January 31, 2026, if they are working in good faith to comply with the prohibition. This grace period allows time for providers to create appropriate systems and policies to comply with the new requirement.

# Next Steps and Recommendations

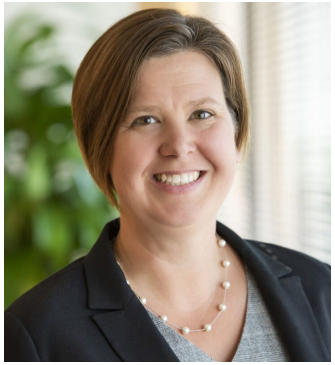
# To Do List

- Evaluate which of these changes impact you
- Review existing processes that may be impacted
- Revise internal policies and procedures
- Update Notice of Privacy Practices
- Assess business associate agreements
- Communicate expectations with workforce and vendors
- Incorporate reminders about these restrictions in training sessions (e.g., annual privacy and security training) for relevant members of the workforce to ensure continued awareness

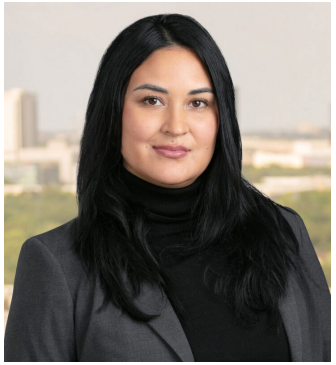
# Deadlines

- The Rule became effective June 25, 2024
- Most compliance with the Final Rule is required by December 23, 2024
- Notice to Privacy Practice changes, which must be implemented by February 16, 2026

# Questions?



**Stacy Harper, JD, MHSA, CPC**
Overland Park, KS
913.327.5120
sharper@spencerfane.com



**Christine Chasse, JD, MSN, RN**
*Plano, TX*
214.459.5884
cchasse@spencerfane.com



SpencerFane

# CLE December 9th, 2024  Health Law Navigator: Privacy Updates

| State | Credit Type |
|---|---|
| Arizona | 1 General |
| California | Pending |
| Colorado | 1  General |
| Florida | 1 General |
| Kansas | 1 General |
| Minnesota | 1 General |
| Missouri | 1.2 General |
| Nebraska | 1 General |
| Nevada | 1 General |
| New Mexico | 1 General |
| Oklahoma | 1 General |
| Tennessee | 1 General |
| Texas | 1 General |
| Utah | 1 General |

**Note: The CLE credit hours displayed are based on attendance for the entire series. Partial credit will be granted for attendance at individual sessions.**

*If you would like to request CLE's and did not provide your bar number during registration, please email your bar number to education@spencerfane.com.*
*Please allow 7-21 days to process CLE credits. While sessions are recorded and available for 30 days, many states have restrictions regarding on-demand sessions.*
*Our recordings do not meet all state requirements. To receive credits for on-demand viewing would require self-submission to your state bar and thorough understanding of that state's requirements.*

SpencerFane