Clark Hill

Navigating the Where, When, and What of Data Privacy Risk Assessments

January 20, 2026

Authors

Jason M. Schwent , Hannah Donahue

As noted in last week's post, privacy risk assessments are now required in several states. Of the 19 U.S. states with comprehensive consumer data privacy laws, all but two mandate that businesses conduct privacy risk assessments when processing of consumer personal information in ways that could pose a risk to consumer's privacy.

These assessments are not simple checklists—they involve detailed analyses weighing the risks of collecting and processing information against the benefits to the business, considering the safeguards the business plans to implement. Performing these assessments carries significant regulatory implications and potential litigation risks. These important topics will be discussed in next week's post. Before we get there, this post discusses the key threshold questions—**WHERE**, **WHEN** and **WHAT**—to determine whether a privacy risk assessment is required So the question becomes, when do businesses need to conduct one of these risk assessments?

WHERE are Data Privacy Risk Assessments Required?

The first step is determining whether your business falls under one of the 17 state consumer data privacy laws that require privacy risk assessments. Currently, these states mandate assessments under certain circumstances: **California, Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia**. In addition, 7 states—**Maine, Massachusetts, Michigan, New York, North Carolina, Pennsylvania, and Vermont**—have active bills in their legislatures that would impose similar requirements. Ten other states (Georgia, Hawaii, Illinois, Oklahoma, South Carolina, Washington, West Virginia, and Wisconsin) have

previously introduced bills on this topic, even though those measures did not pass. In total, 34 states have either adopted, are considering, or have recently considered legislation requiring data risk assessments requirements. If you operate in or are actively pursuing business in any of the 17 states with existing requirements—or the 7 states currently considering such laws—you should understand WHEN these assessments apply and WHAT the triggering activities are.

Beyond U.S. state laws, business in the European Union must comply with the General Data Protection Regulation (GDPR), which also requires privacy risk assessments. Similarly, covered entities or business associates under HIPAA must conduct annual risk assessment of their data privacy practices.

In short: If you operate in or do business in any of these 24 U.S. states, the EU, or are covered by HIPAA, you are either already—or likely soon will be— required to conduct data privacy risk assessments.

WHEN Is a Risk Assessment Required?

Except for annual HIPAA assessments (and excluding those HIPAA risk assessments triggered by significant operational changes), whenever a specific action requires a risk assessment, that assessment must be conducted *before* the activity begins. This means risk assessments must be considered during the earliest stages of project development to ensure they are finalized well in advance of any data collection.

While regulators likely will not have reason to request these assessments prior to collection, issues such as security incidents or a consumer complaint can change that. If an investigation reveals that personal information was collected before a risk assessment was performed and documented, regulatory penalties may follow. Further, in litigation related to a security incident, failing to conduct a risk assessment before collecting the affected personal information could impact arguments about liability.

WHAT Activities Trigger a Risk Assessments?

Each law—whether a state law, EU regulation, or federal requirement—defines specific circumstances that trigger the need for a privacy risk assessment. Under U.S. state laws, triggers vary by jurisdiction.

California

Businesses must conduct a risk assessment before engaging in any activity that presents a “significant risk to consumers’ privacy.” This includes:

- Selling or sharing personal information;

- Processing sensitive personal information;
- Using automated decision-making technology (ADMT) to make a significant decision about consumers;
- Using automated tools to infer or analyze traits based on systematic observation of employees, job applicants, or students;
- Processing personal information to train ADMT for purposes like emotion recognition, biometric profiling, or significant decision-making.

Colorado, Texas, and Virginia

These states require a risk assessment when there is a "heightened risk of harm," which includes:

- Targeted advertising or profiling that could lead to:
  - Unfair or deceptive treatment or unlawful discrimination
  - Financial or physical injury
  - Offensive intrusion into privacy
  - Other substantial consumer injury;
- Sale of personal data; or
- Processing of sensitive data.

HIPAA

Under HIPAA, covered entities and business associates must conduct

- An annual risk assessment of their practices and procedures; and
- Additional assessments when there are significant operational changes, regulatory updates, or following a security incident.

The bottom line is that businesses that sell or process sensitive data—or personal data in connection with ADMT—must pay close attention to privacy risk assessment requirements. This is especially critical for organizations operating in or serving consumers in the 24 states where such laws are in effect or under active consideration.

These risk assessments are not mere "check-the-box-type" exercises. Regulators have indicated that they view these risk assessments as a serious compliance obligation.[1] Failure to conduct and properly document these assessments can lead to significant regulatory consequences and may also

increase litigation risk.

Now that we've covered the **WHERE**, **WHEN**, and **WHAT** of privacy risk assessments, our next post will focus on the **HOW**—specifically, how to prepare and structure a risk assessment that meets regulatory expectations and minimizes compliance and litigation risks.

If you have questions about your business and risk assessments, let the professionals at Clark Hill help you sort through these regulations and their impact on your business.

[1] *See, e.g.*, Press Release, U.S. Dept. of Health and Human Servs., HHS' Office for Civil Rights Settles HIPAA Privacy and Security Rule Investigation with a Behavioral Health Provider (July 7, 2025), HHS' Office for Civil Rights Settles HIPAA Privacy and Security Rule Investigation with a Behavioral Health Provider | HHS.gov (quoting HHS's OCR Director as observing that covered entities or business associates involved in HIPAA Security Rule enforcement actions "often have deficient risk analysis practices" that commonly include "lacking a risk analysis entirely or failing to update existing risk analyses when implementing new technologies or expanding operations that affect the security of ePHI").

Related Industries

Food & Beverage

Hospitality

Retail