



# Privacy: The ongoing trend of new data protection laws and regulations causes new compliance minefields and other legal risks

## PRIVACY TRENDS:



In the U.S., privacy and cybersecurity-related enforcement is expected to increase.



In Europe, managing international data transfer restrictions will be a key focus, and additional guidance is expected to be published on areas of digital health such as AI.




In China, new laws and forthcoming guidance will have a significant impact on how life sciences companies process data.



Cybersecurity attacks on life sciences companies are likely to increase.






An uncertain and rapidly evolving data protection landscape means that life sciences companies must pay increasing attention to privacy issues. Data breaches are now more complex, frequent, and impactful, and the cost of these breaches has grown significantly in just the last year.

Policymakers in many countries are having nationwide conversations about data subject rights. Evolving privacy laws pose particular challenges to life sciences companies with global operations, because a major focus of these laws is to regulate cross-border data transfer. Life sciences companies are also being affected by evolving privacy laws across the wider data economy.

In the U.S., regulators are increasingly interested in bringing privacy and cybersecurity-related enforcement actions, and the class action plaintiffs' bar is very active. Preparations for new privacy and cybersecurity requirements that will come into effect in 2023 from state laws in California, Colorado, and Virginia are underway. The development of new regulations in California, and other interpretive guidance or regulators for state laws, as well as potential new HIPAA regulations or guidance, will be a major focus throughout 2022. It is also very possible we will see additional U.S. states pass their own privacy laws during the coming year, and Congress continues to seriously consider federal legislation.

In Europe, issues around data privacy will only become more challenging for life sciences companies during 2022 as concerns around international data transfers continue to evolve. This will create a need to carry out data transfer assessments and put in place new European data transfer agreements. More guidance is expected to be published on areas of digital health, such as AI. Ransomware attacks and other forms of cybersecurity attacks are likely to increase and will be of key concern to life sciences companies.



Last year, China took the major step of introducing a Data Security Law (DSL) and a Personal Information Protection Law. Both impose severe penalties for infractions and will have a significant impact on how life sciences companies process data. In 2022, China is expected

to publish specific regulations and guidance to support the implementation of the new laws. These will include a regulation on security assessment for cross-border data transfer, a China-version standard contractual clause for the cross-border transfer of personal data, and a catalogue of important data that is subject to the DSL.

## PRIVACY TIPS:

- As data ethics come more clearly into focus, companies should build data governance programs covering not just existing privacy laws but also extra-legal considerations.
- Life sciences companies should closely monitor U.S. state privacy law developments, as well as distinctions in HIPAA and clinical trial exemptions among state laws.
- In Europe, additional resources will be needed to carry out the required international data transfer assessments and to put in place new European data transfer agreements.
- Life sciences companies with activities in China must closely monitor data privacy regulatory developments. Some data in the healthcare industry may become regulated as “important data,” and those processing it will be subject to enhanced security obligations under the DSL.

## Contacts

[Colleen Brown](#), [William Long](#), and [Chen Yang](#)