

Responding to CCPA, GDPR and the Tumultuous World of Data Privacy

A photograph of a business meeting. In the foreground, a person's hand is holding a pen over an open notebook. To the right, another person's hand is pointing at a laptop keyboard. The background shows other people in business attire, slightly out of focus. The overall scene is professional and focused on data and technology.

November 6, 2019

Welcome



Adam Greene, JD, MPH

Partner and Co-chair, Health Information & HIPAA Practice, Davis Wright Tremaine LLP; Former Senior Health Information Technology and Privacy Specialist, Office for Civil Rights, HHS, Washington, DC (Co-moderator)



Rena Verma, MBA

Senior Managing Director, Information Governance, Privacy and Security Practice, FTI Consulting, New York, NY (Co-moderator)



Jennifer Chillas, JD

Senior Corporate Counsel, Bristol-Myers Squibb, New York, NY



Catherine Williams, JD

Director, Privacy Office, Novo Nordisk; Former Assistant General Counsel, Privacy & K-12, Corrections & Leisure, Aramark, Plainsboro, NJ

The views, information or opinions expressed during this session are solely those of the individuals involved and do not necessarily represent those of their employers or any associated committee, group or individual.



Overview

This session will cover the practical issues that data privacy officers are dealing with on a day to day basis to address the rapidly evolving data privacy regulatory landscape in the US and the EU.



The Old ... HIPAA

- Only applies to covered entities and business associates, which often do not include pharmaceutical companies.
- Generally limits sharing of protected health information from health care providers to pharmaceutical companies without patient consent.
- HHS is working on amendments to HIPAA regarding:
 - Potentially shorter deadline for providing patients access to their information.
 - Improving ability to share for care coordination
- A focus of current HIPAA enforcement is greater patient access to their information.



Improved Patient Access

- HHS is working on giving patients greater access to their electronic health information, including through apps, and prohibiting information blocking.
- Potential to make it significantly easier for patients to share obtain and share their information for research purposes.



The Old ... 42 C.F.R. Part 2

- Regulations governing substance use disorder patient records.
- Even older than HIPAA, but has been amended in 2017, 2018, and there is a current notice of proposed rulemaking.
- A key privacy regulation with respect to efforts to combat the opioid crisis.
- Includes permission for disclosure for research if recipient bound by HIPAA or HHS Common Rule.
 - Otherwise, a very challenging consent requirement is applicable (which currently requires naming a specific individual recipient, rather than an entity).



The Old ... The FTC

- Section 5 of the FTC Act prohibits “unfair” and “deceptive” trade practices.
- A violation of a privacy policy is treated as deceptive, and poor information security practices may be either.
- Standard resolution is a 20-year consent order.
- Very interested in privacy and security of health information that falls outside of HIPAA, such as consumer genetic testing and health-related apps.

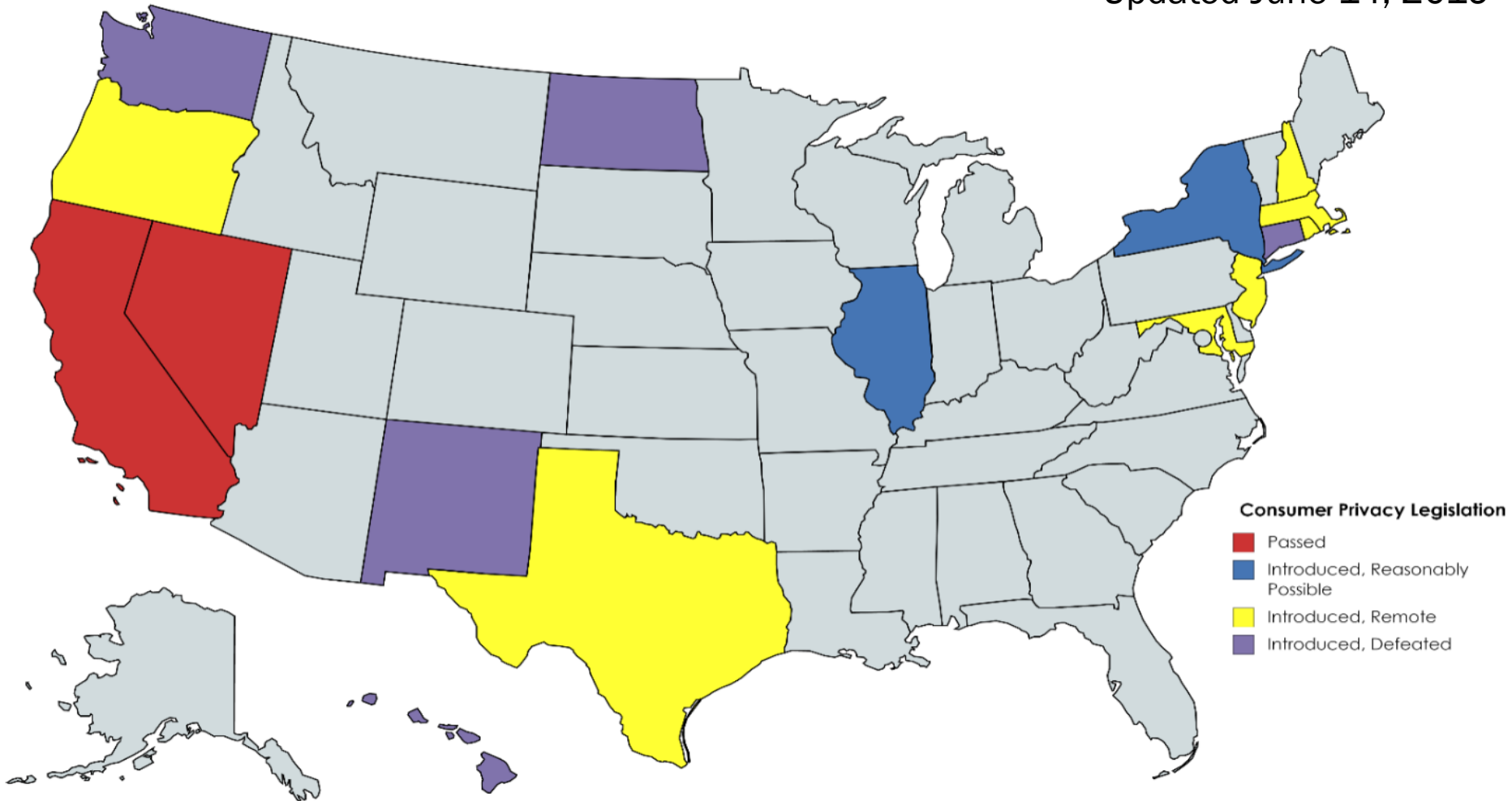


The Newish ... GDPR

- Effective May 25, 2018
- Potential triggers:
 - Operating in EU (including clinical trials)
 - Targeting EU data subjects
 - Monitoring EU data subjects (e.g., online tracking)
- 12 major fines in 2018 and 2019, resulting in **€359,205,300** (source <https://alpin.io/blog/gdpr-fines-list/>)

The New ... State Privacy Laws

Updated June 14, 2019



The New... CCPA

California Consumer Privacy Act

The law applies to companies that do business in California and meet one or more of the following:

1. annual gross revenues exceeding \$25 million;
2. buys, receives, sells or shares the personal information of 50,000 or more California consumers, households or devices;
3. derives 50 percent or more of its annual revenues from selling consumers' personal information.

“Now is the time to assess the impact of the law to your business, understand the obligations and begin taking steps to modify processes accordingly.”





Components of Current Draft CCPA

- Definition of “sale”—as the disclosure or availability of personal information for monetary or other valuable gain
- Inclusion of “household”—the law’s definition remains ambiguous, and may encompass an individual, residence, family, device or group of devices
- Enhanced privacy notice requirements
- The consumer’s “right to opt out” of any sale of their data
- The individual’s right to access, including the right of disclosure, portability and deletions
- The right to equal service and prices (*no retribution or price premiums for “privacy-equipped” services*)
- Right to be informed of categories of personal information that a business collects, receives, sells or discloses; purpose of activities; and categories of parties disclosed to
- New fines enforceable by the California Attorney General, including civil penalties of up to \$2,500 for unintentional violations and up to \$7,500 for intentional violations
- Private rights of action for breach events of nonencrypted or nonredacted personal information
- An initial framework for “financial incentive programs”
rewarding consumers that permit the sale of their data



GDPR Similarities

As many multi-national organizations have already experienced, the **EU's GDPR fundamentally changed the way many businesses manage personal data.**

The CCPA is similar to GDPR in numerous ways, providing **privacy rights centered around notice, access and consent** for California residents.

It will introduce **new fines for non-compliance** and lawsuit parameters for residents impacted by illegal processing or mishandling of their data.

Organizations that have already implemented privacy-driven changes for GDPR will have a head start. These corporations can take learnings and programs they have deployed in Europe, and apply them to California resident data. But U.S.-based **companies that have not dealt with operationalizing data privacy or GDPR compliance will face some heavy lifting** to implement the information governance and privacy programs necessary to meet CCPA's requirements.



How to Prepare

1. Map your data

Prepare a clear map of where the organization stores personal data (across digital and hard copies), for how long, and how that data is used or shared with other parties; be sure to include an extensive understanding of the regulatory risk exposure with respect to that data and how the compliance obligations impact products, services, business processes, internal systems, external third-party relationships, etc.

2. Update privacy notices

Work with counsel and privacy experts to develop compliant notices that include 1) a description of consumer rights under the law, 2) a comprehensive list of third parties to whom the business sells personal information, 3) categories of third parties to whom the business discloses personal information for business purposes. Privacy notices must be in place by January 2020 for consumers and by January 2021 for employees.

3. Identify and document personal data “sales”

Provide clear and conspicuous consent requests and a “Do Not Sell My Personal Information” link on your website homepage. Implement a process for handling do not sell requests and make it easy for consumers to navigate. Review vendor contracts to ensure that the sale/use of personal information is limited within the confines of the law, and that data rights requests implicating this information can be responded to and executed in a timely manner.



How to Prepare

4. Prepare to respond to data rights requests




Provide a toll-free telephone number and/or email address where individuals may submit data access requests and/or privacy complaints. Responding to these can require substantial effort. Develop a standardized workflow for fielding requests within the designated 45-day timeline. Prepare an outline for data subject requests that includes authenticating the person(s) making the request and process flow for handling access and deletion of data according to the request. Similarly, have a plan in place for intake and response for privacy complaints.

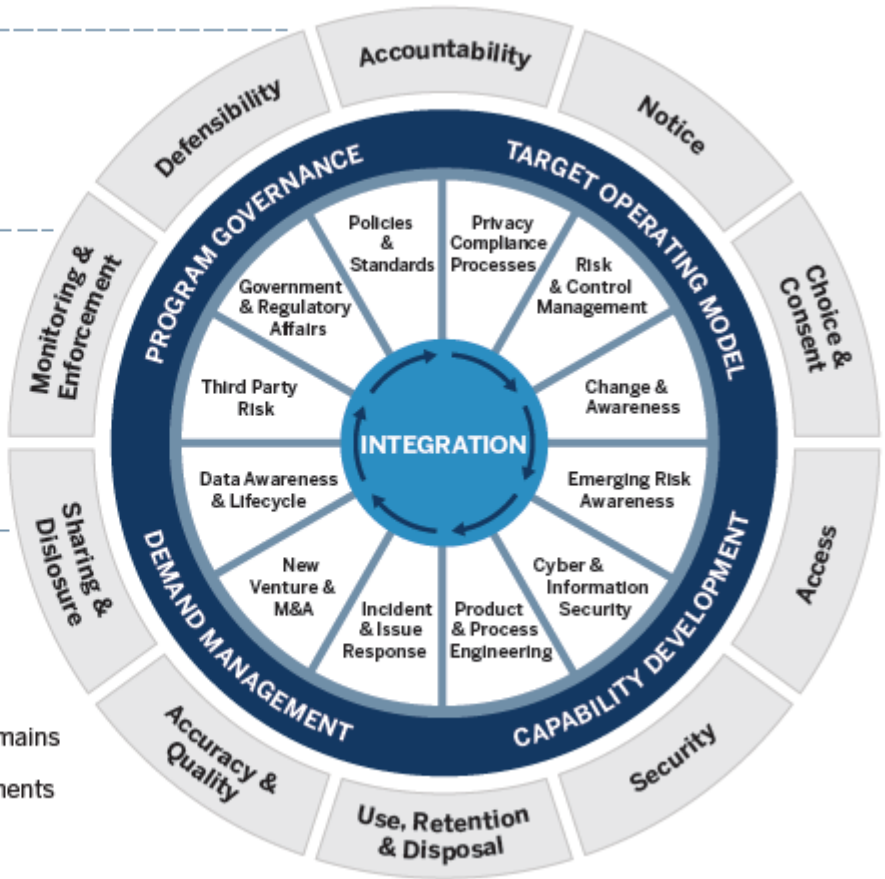
5. Implement and commit

Smooth implementation is extremely important, but it can end up in vain if the privacy compliance control environment is not preserved and sustained. Resources and budget must be allocated commensurate to the organization's risk, with separate program resourcing and budget built in to sustain compliance over the long term. Non-compliance comes with a bottom line impact, but so does "over compliance." Taking time to calculate sufficient budget and resourcing, then committing to the spend will help keep privacy program owners accountable to deliver upon the defined risk tolerance. It takes time, material and experienced people to affect data privacy.

Privacy Data Framework

- 
 Modular domains that can scale commensurate to risk appetite, strategic priorities, and domain maturity.
- 
 Comprehensive yet targeted definition of privacy's reach within the organization.
- 
 Future-proof, regulation-agnostic, and risk-based.
- 
 Maps to common organizational risk ownership putting integration activities at its center.

-  Privacy Capability Domains
-  Management Components
-  Privacy Principles



A holistic, outcome-based model intended to cover all aspects of a company's data privacy risk management capabilities.*

*FTI model

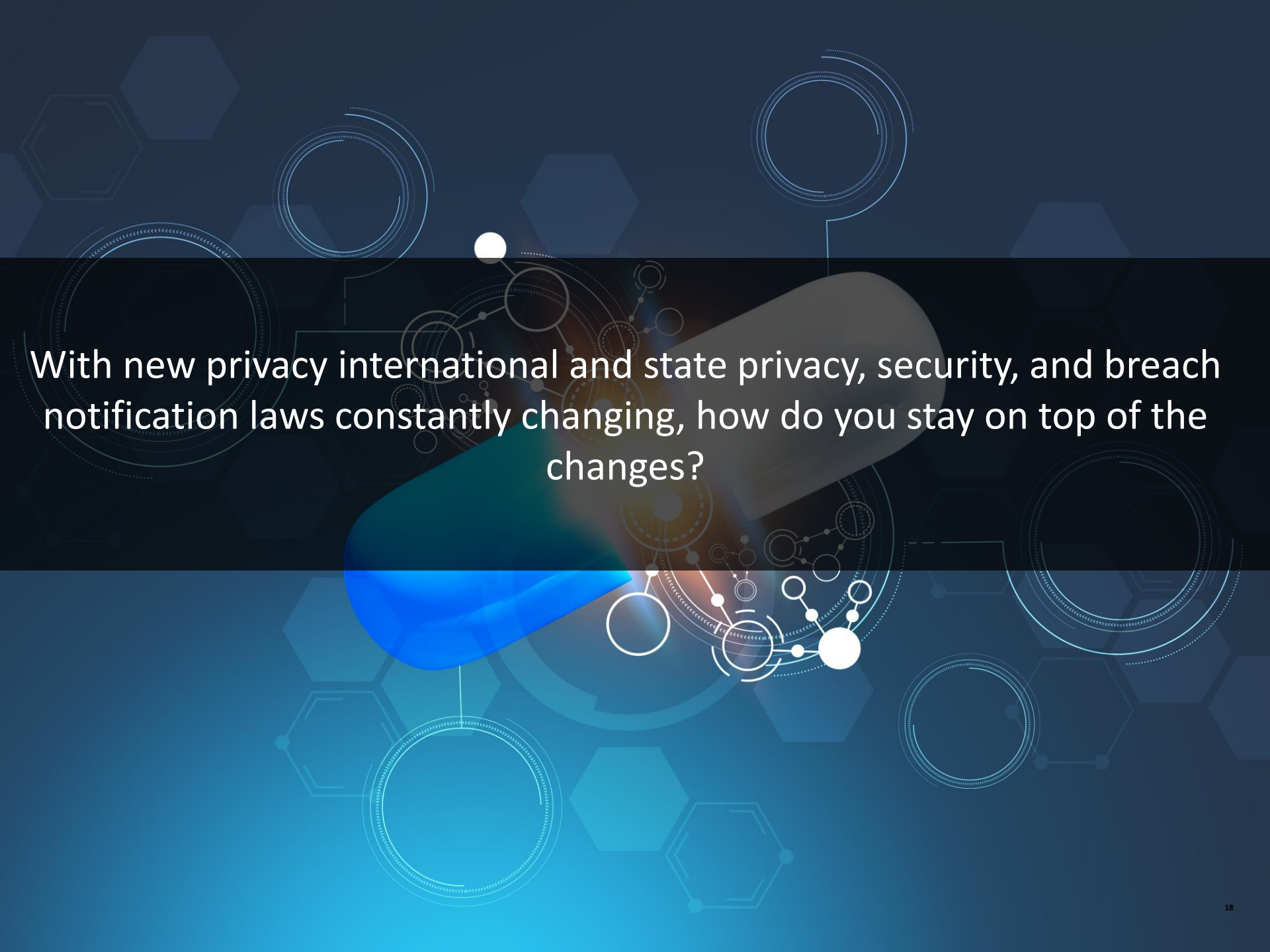


Data Privacy Vendor Landscape

Explosion of Data Privacy Technology providers

- According to the 2019 Privacy Tech Vendor Report by the IAPP, there are currently over 250 Privacy Technology Providers
- Two Main Categories are: Privacy Program Management and Enterprise Privacy Management, which include tools for
 - PIA Assessment tools
 - Consent Management
 - Data Mapping
 - Incident Response
 - Activity Monitoring
 - Data Discovery

The most likely new technologies to be purchased by data privacy officers in the next 12 months are ***data mapping, data discovery and assessment tools.***

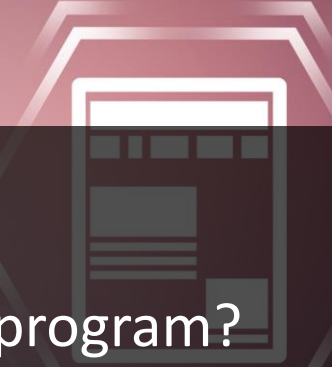
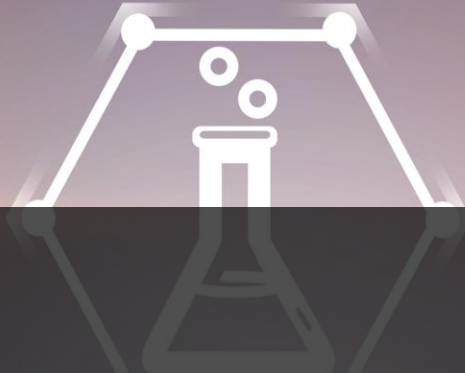


With new privacy international and state privacy, security, and breach notification laws constantly changing, how do you stay on top of the changes?

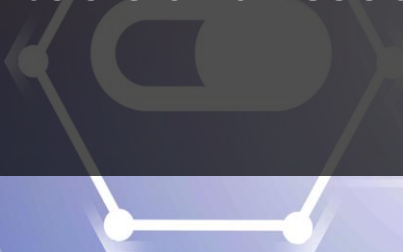
For better or worse, one of the key elements of privacy is a public-facing privacy notice. The FTC has pretty high expectations, and then GDPR and CCPA have each added requirements. How do you manage your privacy notice? How often do you find yourself updating it? How do you balance the legal side with readability?

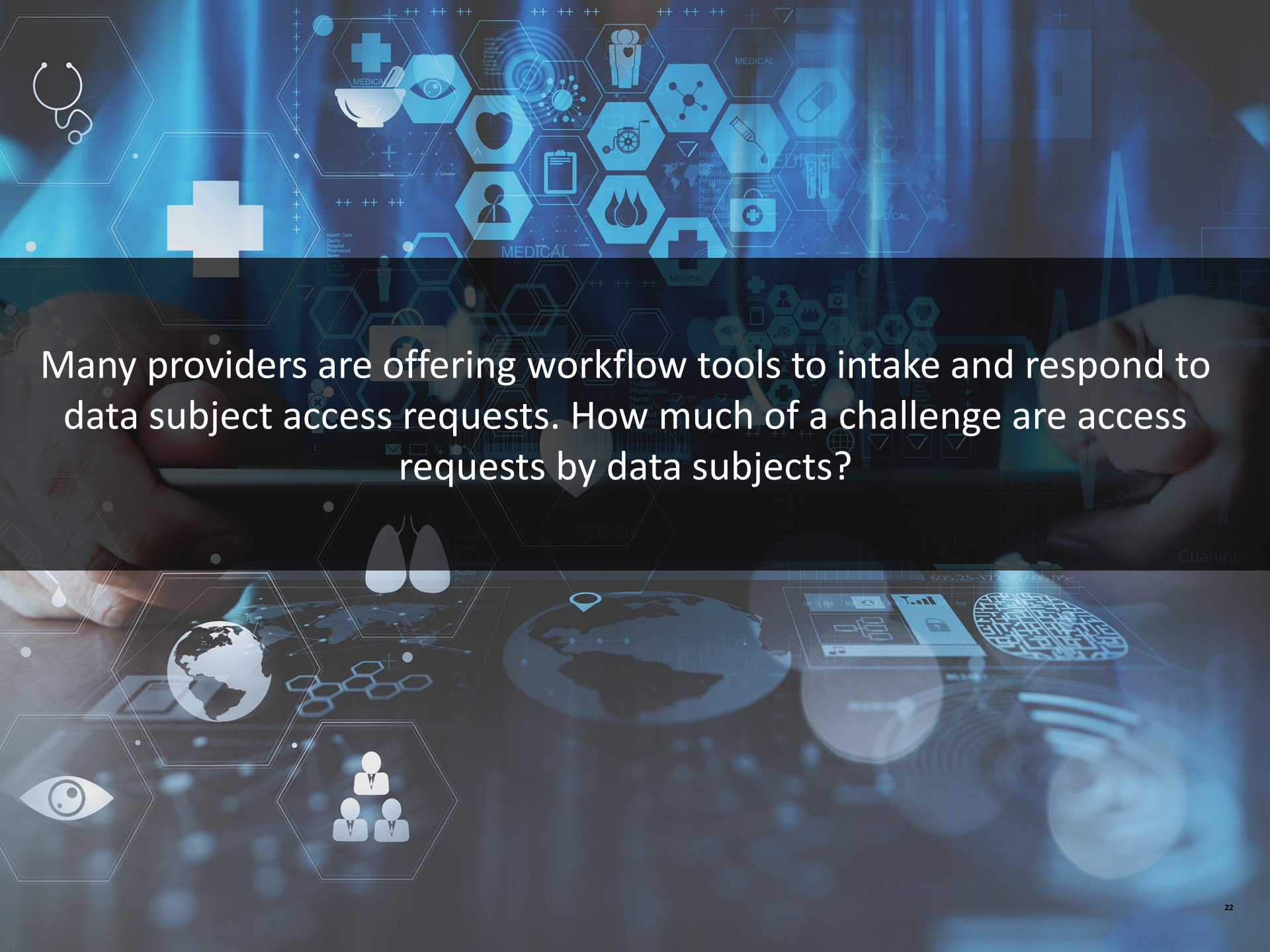


Pharma and the healthcare sector are not new to data privacy with compliance obligations under HIPAA. What should the privacy professionals at pharma and medical device companies focus on as they try to make sense of how the GDPR and CCPA apply to them? What are the most pressing priorities towards achieving compliance?




How important is data mapping to a privacy compliance program?
What kind of tools and resources are you seeing used in this area?






Many providers are offering workflow tools to intake and respond to data subject access requests. How much of a challenge are access requests by data subjects?



How do you see the role of the privacy officer, privacy counsel, security officer, and compliance officer fitting together on a good day? What are their roles on a really bad day – a breach incident?



Any recommendations for how privacy professionals should effectuate privacy-by-design in their organizations, getting involved early rather than receiving last-minute requests for approval?

How do you recommend getting appropriate budget and executive support for privacy initiatives?



Questions?