Managing Consumer Health Data in Compliance with Washington's "My Health My Data" Law

Presenter: David Ritter, CEO of Privacy Lock, a WSCA Corporate Partner

**Disclosure: this presentation and the information provided during this webinar is not intended to, constitute legal advice; instead, all information, content, and materials available on this site are for general informational purposes only.*

Our Experience with Privacy Regulations

NIST Privacy Workforce Public Working Group

Colorado Privacy Policy Commission

UNIVERSITY of WASHINGTON

iapp

WSCA WASHINGTON STATE CHIROPRACTIC ASSOCIATION

www.myprivacylock.io

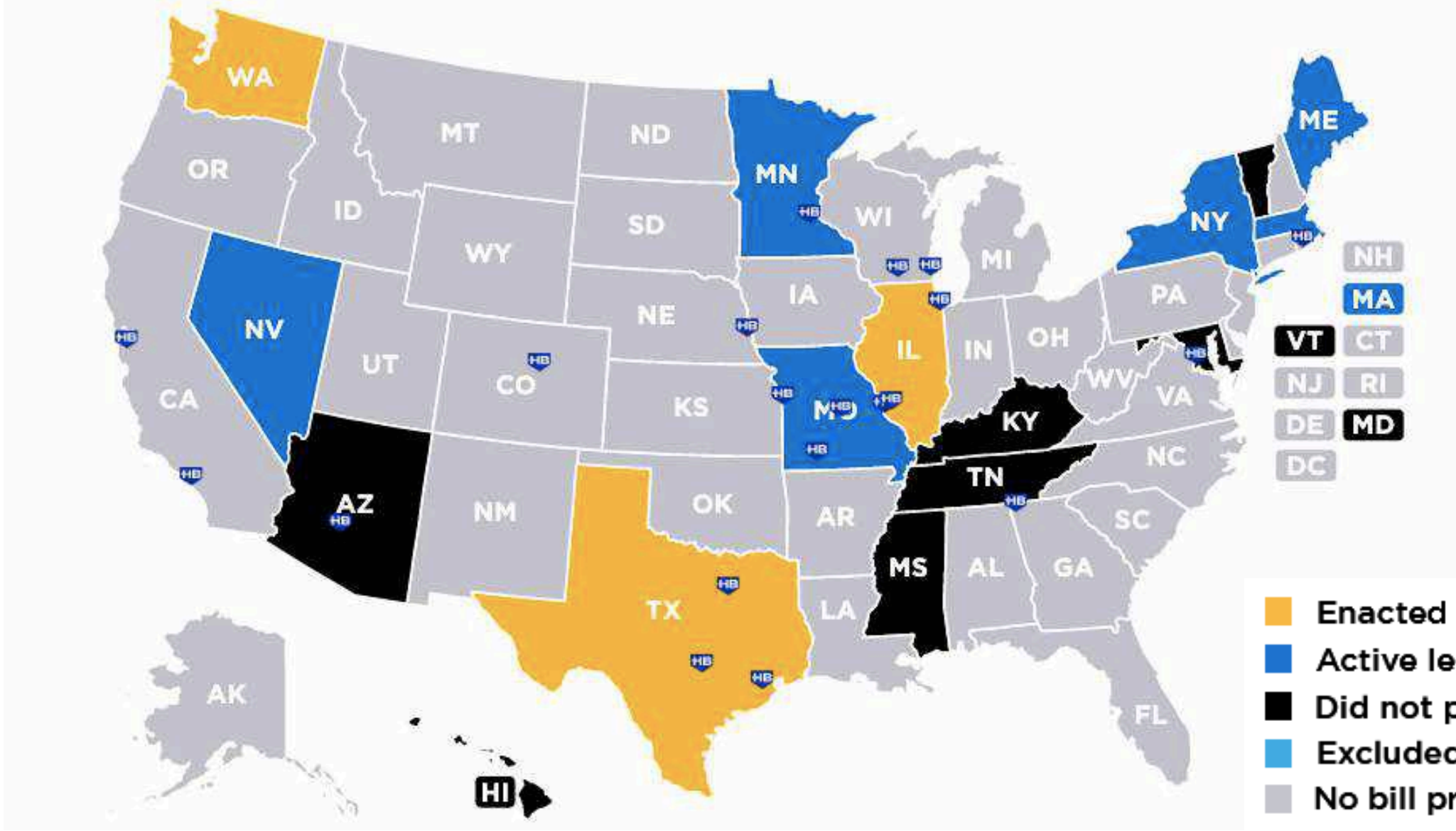
New U.S. Privacy Regulatory Landscape

13 states have consumer privacy laws.

3 states have new health/ biometric privacy laws.

State Privacy Tracker - 2023

Biometric Data and Health Data Laws



Washington passes nation's first health-data privacy law

Washington's "My Health, My Data" act provides consumer protections not found in the Health Information Portability and Accountability Act.

BY KEELY QUINLAN • APRIL 27, 2023

Important Details of MHMD

No exemption for non-profits or small businesses

Limited exceptions to Deletion requests

Includes private right of action

MHMD Effective Dates

March 31, 2024 for regulated entities

June 30, 2024 for small businesses

Who Is Required To Comply?

Under MHMD, a "regulated entity" is defined as a legal entity that:

- Does business in Washington; and
- Determines the "purpose and means of collecting, processing, sharing, or selling consumer health data."
- Small businesses are regulated by MHMD and must comply by June 30, 2024. There is no minimum number of data subjects or revenue threshold to fall within its scope.
- MHMD has no revenue thresholds, no minimum number of consumers and generally no entity-level exemptions (for example, nonprofits and entities subject to other federal or state privacy laws)
- MHMD excludes government agencies and tribal nations.
- Based on the definition of "consumer health data," MHMD may apply to a non-traditional healthcare organizations – app providers, OEMs, retail stores, informational websites, platforms, etc.

Definition of Consumer Health Data

"Consumer health data" is defined in MHMD as:

- Personal information that "identifies or is reasonably capable of being associated or linked, directly or indirectly, with a particular consumer."
- Information that "identifies the consumer's past, present, or future physical or mental health status."
- MHMD Act does not define consumer health data in relation to diagnosis or treatment by a medical professional.
- The law also applies to non-health data that can be used to re-identify individuals and tie them to consumer health data. (Algorithms, AI, proxy, derivative data, could be included as CHD).
- MHMD's definition of "personal information" includes "data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.

MHMD Obligations at a Glance

1. Maintain a consumer health data privacy policy.
2. Opt-in consent for certain data collection and sharing.
3. Comply with data subject access requests (DSAR)
4. Maintain reasonable data security measures.
5. Establish data processing agreements with processors.
6. Do not sell consumer data without "valid authorization" from consumers.
7. No "geofence" around an entity that provides in-person healthcare services under certain conditions.

Disclosure requirements in privacy policies

1. The categories of CHD, and the purpose(s) for which the regulated entity collected the data and how it will use such data.

2. The categories of sources from which the regulated entity collected the data.

3. A list of the categories of third parties and specific affiliates with which the regulated entity shares data.

4. The categories of data the regulated entity shares.

5. How consumers can exercise their rights under the MHMD.

Consumer Health Data Privacy Policy

A business covered by MHMD is required to place a link to its Consumer Health Data Privacy Policy on the company's homepage.

Purpose Limitation

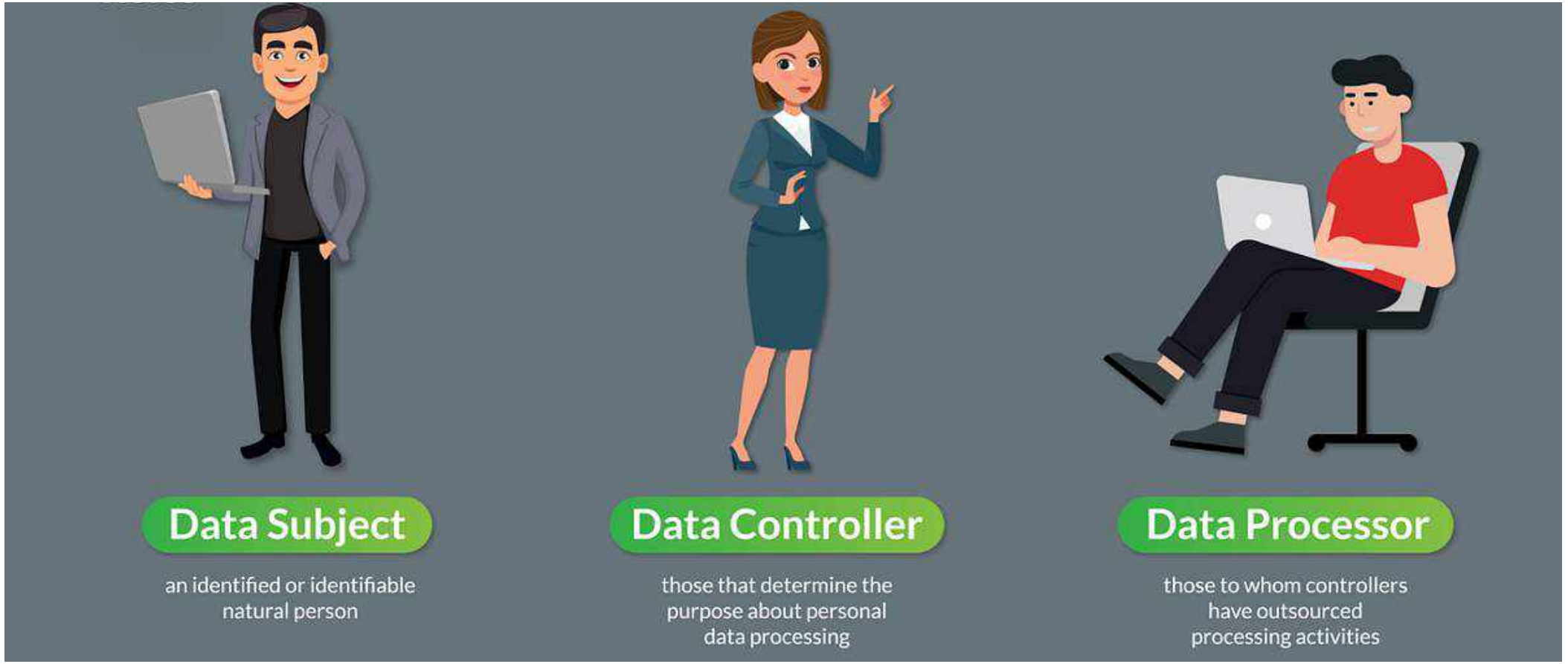
Entities are barred from collecting, using or sharing consumer health data, or additional categories of such data, for purposes not disclosed in the health data privacy policy without first disclosing the additional purposes and obtaining affirmative consent from the consumer. Processors may process consumer health data pursuant to a binding contract that sets forth processing instructions and limits the actions a processor may take with that data.

Purpose Limitation Takeaways

Be explicit about the kinds of data you collect, the types of processing, and what you share with third parties.

Execute agreements with your third party data processors that are consistent with your disclosures and privacy policies.

Converting Vendors to ‘Processors’ under MHMD



A **Processor** under MHMD processes consumer health data “on behalf of” a regulated entity. A processor and regulated entity must have a written contract (ie. Data Protection Agreement) that provides “binding instructions” for processing consumer health data. A processor becomes a regulated entity to the extent that it violates any of the regulated entity’s instructions.

Responding to Deletion Requests

- Consumers have the right to request that regulated entities delete their CHD.
- The MHMD does not contain typical exceptions from other consumer privacy laws, such as the ability to retain CHD to respond to legal claims despite receiving and responding to a deletion request.
- Flow Down Requirements: MHMD obligates regulated entities to flow down deletion requests to affiliates, processors and other third parties receiving shared CHD.

What this means: Regulated entities may find it necessary to have a data map to respond accurately to right to know and deletion requests, and will need to assess which deletion requests may be exempted and which require compliance.

Compliance Exemptions

MHMD does not provide for any entity-level exemptions from compliance. But there are some **data-level exemptions,** including:

- protected health information under HIPAA;
- health information used in accordance with Washington's Uniform Health Care Information Act ("UHCIA");
- patient identifying information collected, used, or disclosed in accordance with federal law relating to the confidentiality of substance use disorder records; and
- personal information governed by the Gramm-Leach-Bliley Act ("GLBA"), the Fair Credit Reporting Act ("FCRA"), and statutes and regulations pertaining to the Washington Health Benefit Exchange.

Some Risk Areas to Consider

Undisclosed Data Processing

Cookies and targeted advertising

Undisclosed Data Processing

CRMs and Marketing Campaigns

Third Party Research

Pro Tip: Data-level exemptions only apply to narrow contexts. For example, data collected under HIPAA that is used for any processing outside of the original collection purpose, may fall outside of the HIPAA exemption. One example - any customer information placed into a CRM tool or used for promoting new products and services would likely be required to comply with MHMD.

MHMD Fines for Violations

	Washington MHMDA
Effective Date	March 31, 2024 *June 30, 2024 - small businesses
Fines	Up to $7,500 per violation
Private Right of Action	Yes. Consumers can bring an action for up to triple damages with a cap of $25,000 and attorney's fees.

Becoming Compliant with MHMD

Privacy Policies and Disclosures

Consumer Permissioning and DSAR

Processor Agreements & Regulatory Filings

Becoming Compliant with MHMD

Update your privacy policy for MHMD and provide a link on your website.

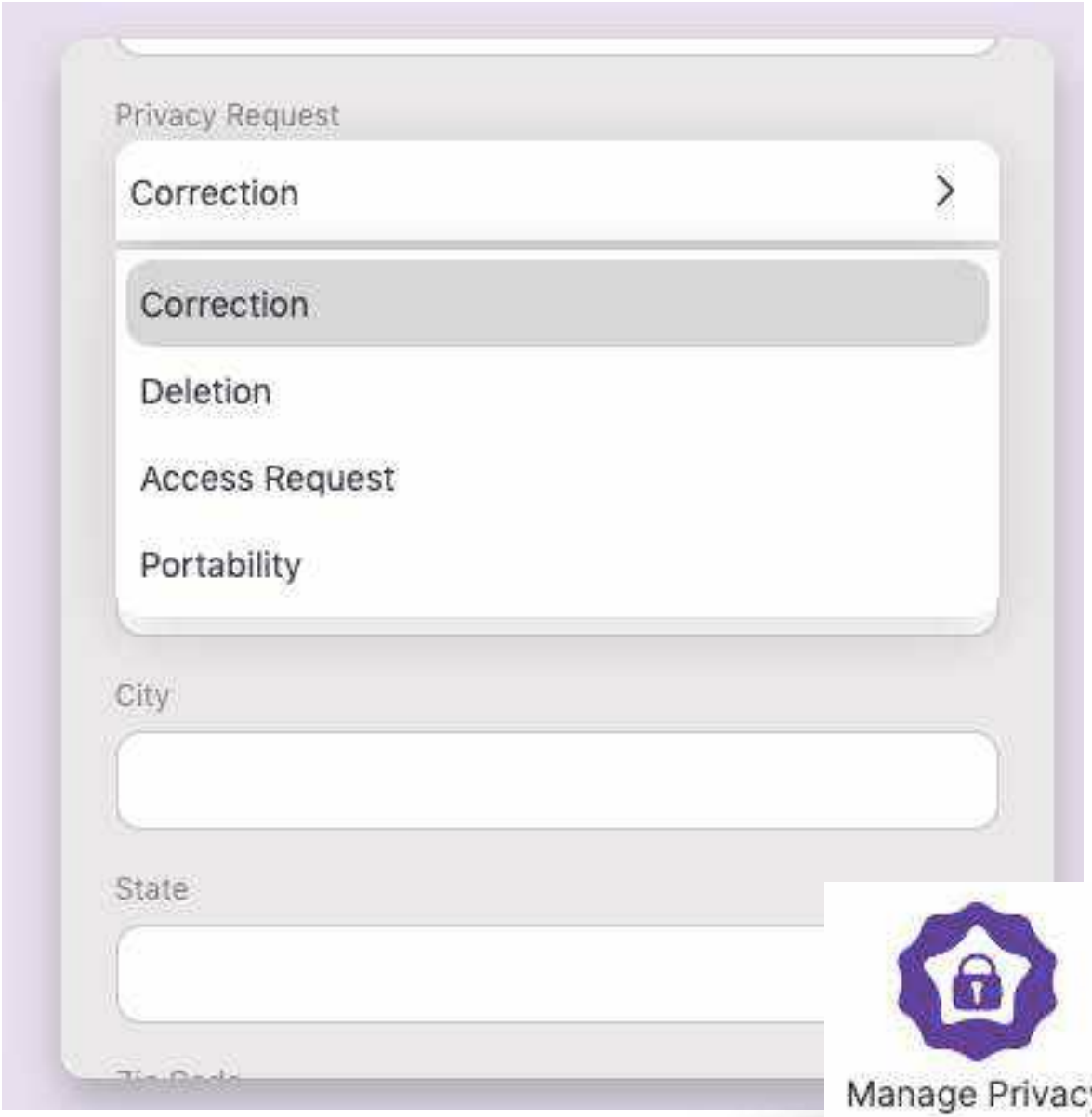
Implement a consumer permissioning program: cookies tracking, DSARs, Opt-In/Out.

Enter into written agreements with vendors that follow MHMD requirements.

Responding to Consumer DSARs

MHMD Data Subject Access Requests (DSAR)

- Right to Deletion
- Right to Know (Access Information)
- Right to Withdraw Consent for Collection/Sharing
- Right to Appeal
- Right to Not Be Denied Services

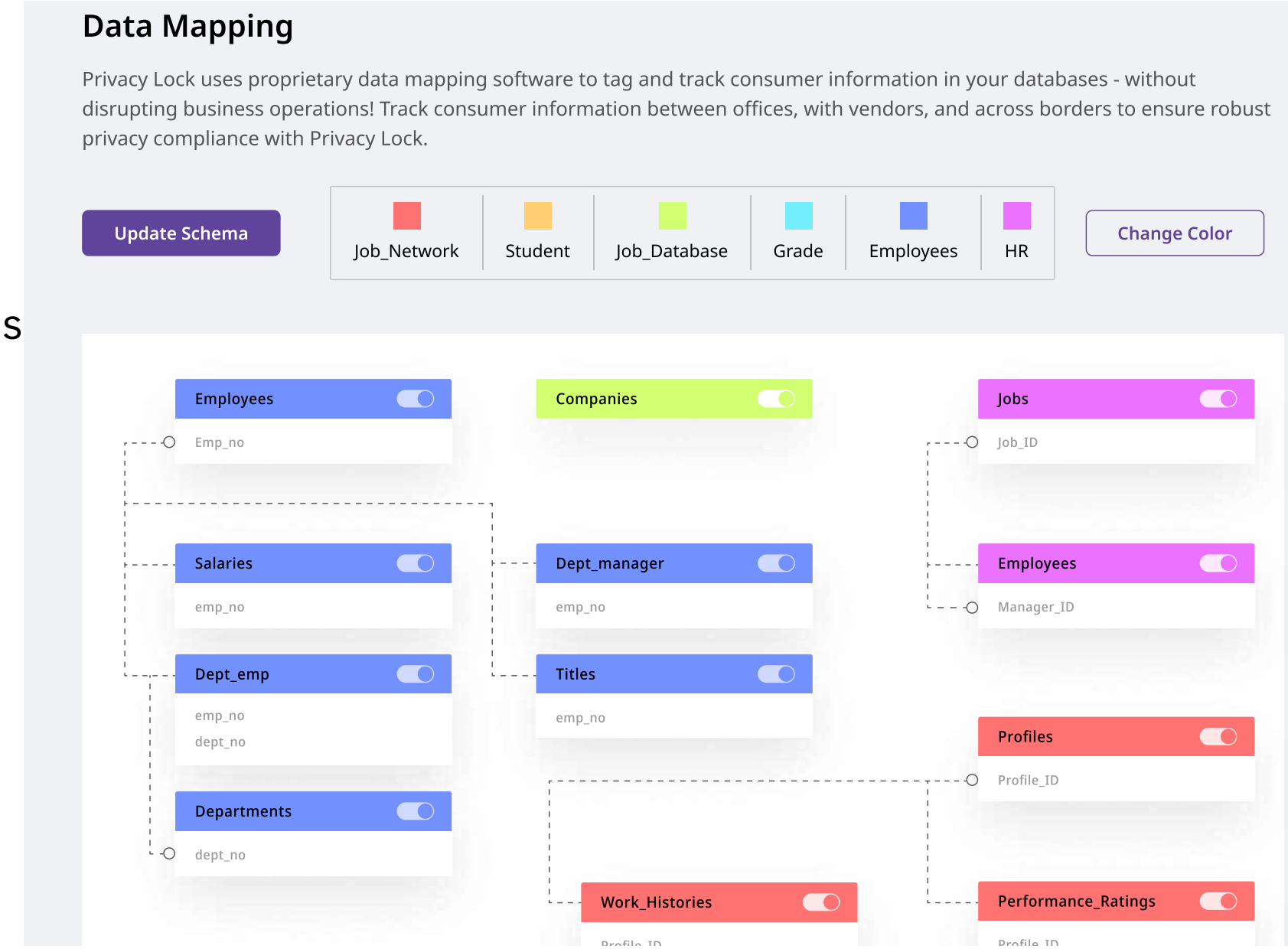


www.myprivacylock.io

Data Mapping and CHD Tracking

- Map your data
- Track data across its lifecycle
- Manage data sharing activities with vendor/processors
- Operationalize consumer permissioning
- Build privacy protocols into your data systems.

www.myprivacylock.io



Getting Your Business Ready for MHMD

1. Know Your Data - identify what data you collect, which third parties have access to it, and what kind of processing you perform on consumer data fields.

2. Conduct an assessment of Privacy Readiness for MHMD.

3. Update your privacy policies for MHMD.

4. Enter into MHMD compliant processor agreements with your vendors.

5. Operationalize privacy: Map Your Data, implement a process for managing consumer consent and DSARs.

www.myprivacylock.io

Let Privacy Lock Be Your Partner in Privacy

Consultation

Privacy Assessment

Tools & Implementation

www.myprivacylock.io

Privacy Lock®

Thank you

Visit us at www.myprivacylock.io