

# Sensitive But Business Critical

## Operationalizing Sensitive Data Consents



Dayle Duran  
Legal Counsel II, Privacy & Security  
Oura



Mason Fitch  
Senior Associate, Hintze Law



Matt Gardner  
Senior Privacy Counsel  
Ro

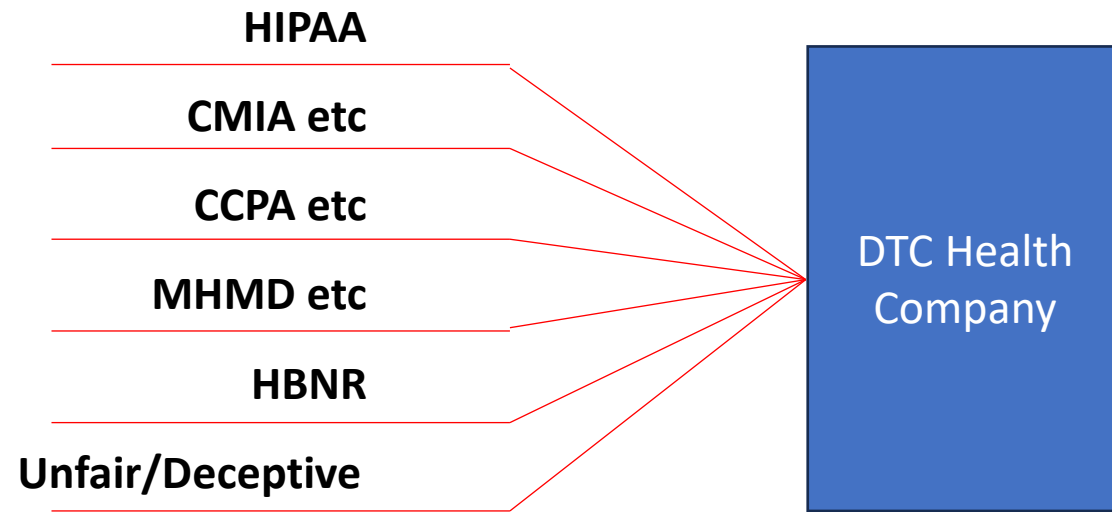


Michael Hamilton  
Senior Director, Privacy  
Adobe

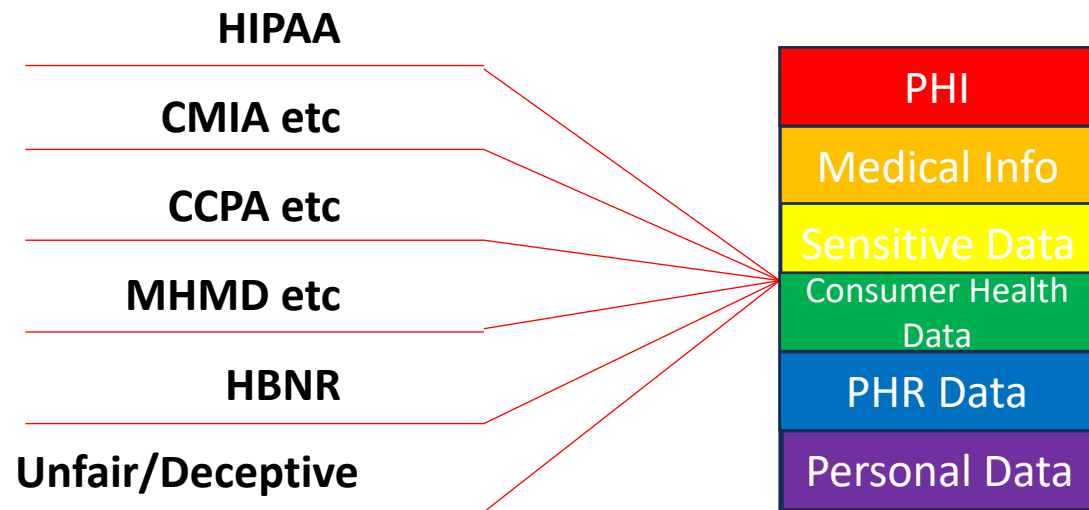
# What we're talking about.

- Why does it matter?
- The current regulatory landscape.
- Defining sensitive data: where is it, and what is it?
- When to ask for consent – and when not to.
- How to ask for consent.

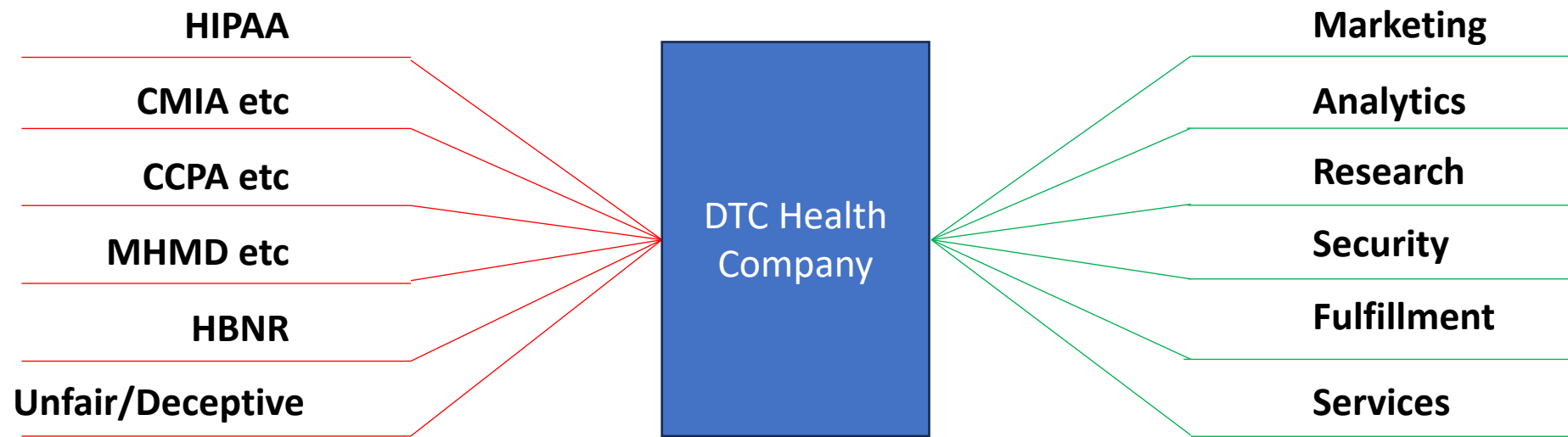
Operating in sensitive data areas is becoming increasingly complicated (especially in healthcare).



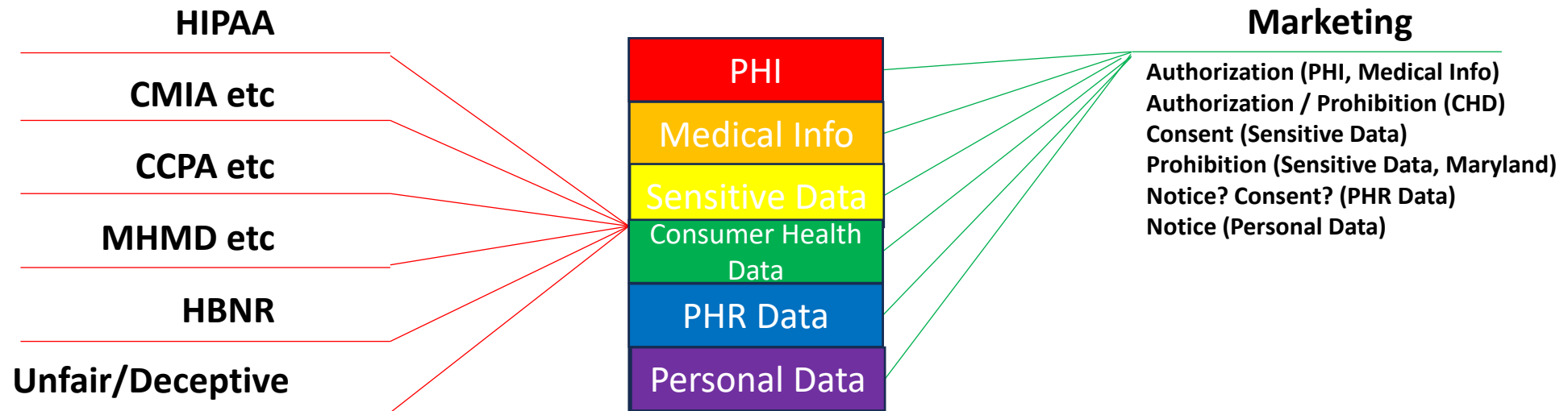
Companies dealing with sensitive data must account for a wide range of laws that apply to different sets of data, at different times, with variations across states.



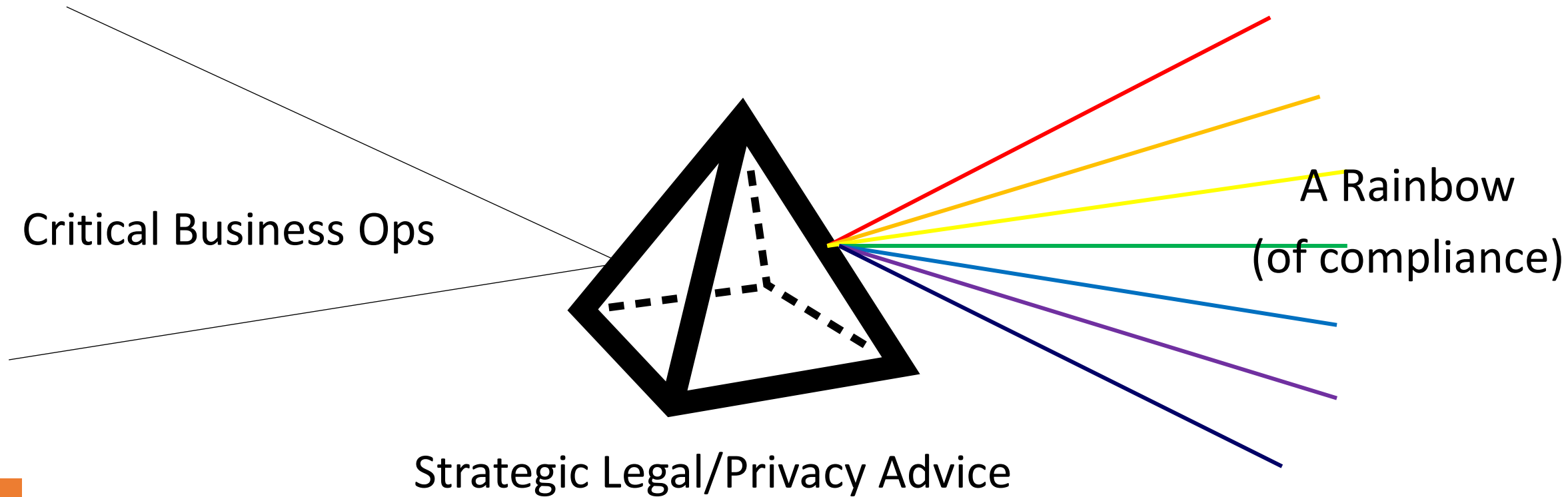
It's more difficult for businesses – especially small and medium businesses – to perform basic functions without overwhelming regulatory burdens.



Especially when single functions can be regulated by several laws, which vary across states.

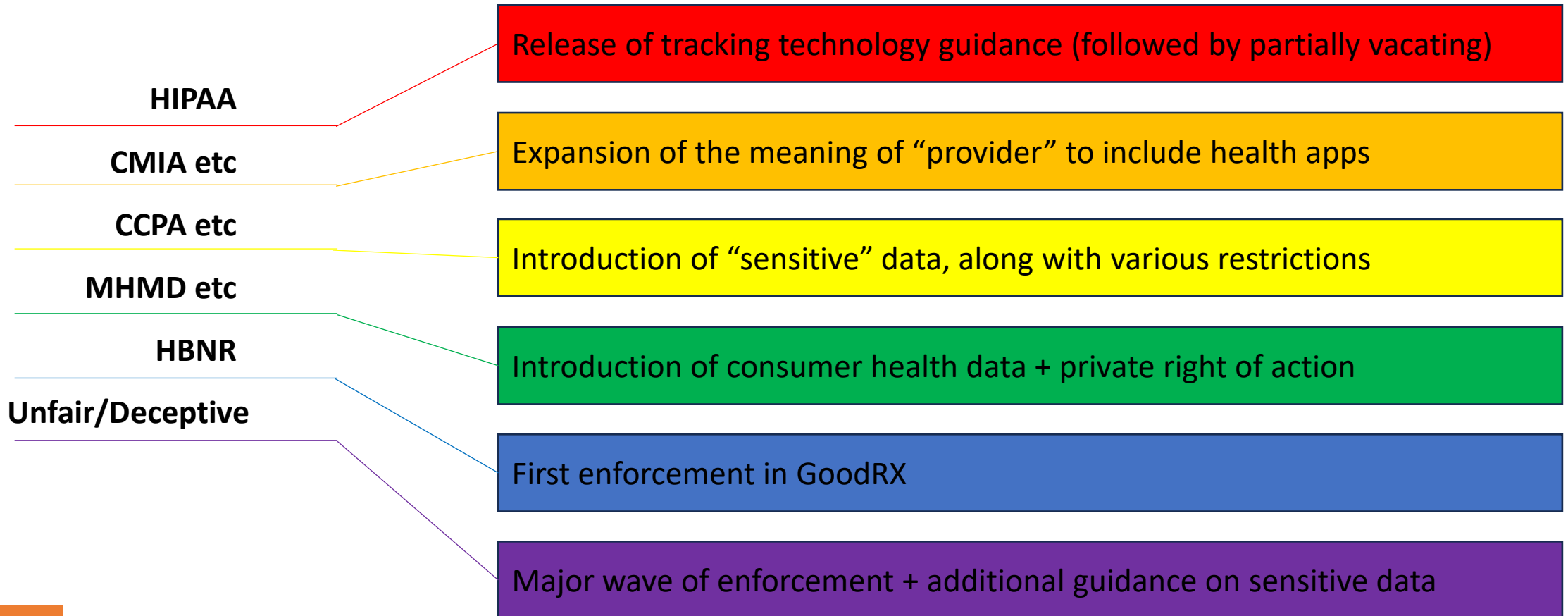


So the question is: how do we support business partners in performing their functions—while complying with the law?





# The regulatory landscape is evolving (quickly).



# The risks are high – but getting it right can be an advantage.

1. Sensitive data can be anywhere.
2. Regulators have signaled that appropriate use and handling of sensitive data is a priority area.
3. Aligning on a strategic approach to good data governance, while still empowering business functions, is critical – and challenging.

# Three key operational considerations:

How do I identify and classify my data?

When do I need to obtain consent?

How do I obtain consent?

## How do I identify and classify my data?

Virginia: Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health **diagnosis**, sexual orientation, or citizenship or immigration status

California: Personal data revealing racial or ethnic origin, religious beliefs, a mental or physical health **condition or diagnosis**, sex life or sexual orientation, or citizenship or citizenship status

Washington: Personal information that is **linked or reasonably linkable** to a consumer and that identifies the consumer's **past, present, or future physical or mental health status**.

# How do I identify and classify my data?

Adopt a  
universal,  
internal  
definition of  
sensitive data

Train your  
workforce  
(actually)

Know your tech  
– and empower  
your people

Build or adopt  
tools

Classify and  
control data

# How do I identify and classify my data?

Adopt a universal, internal definition of sensitive data

Train your workforce (actually)

Know your tech – and empower your people

Build or adopt tools

Classify and control data

- Multi-tiered system vs “least common denominator”?
- State by state or nationwide?
- Track to legal definition or “one size fits all”?

# How do I identify and classify my data?

Adopt a universal, internal definition of sensitive data

Train your workforce (actually)

Know your tech – and empower your people

Build or adopt tools

Classify and control data

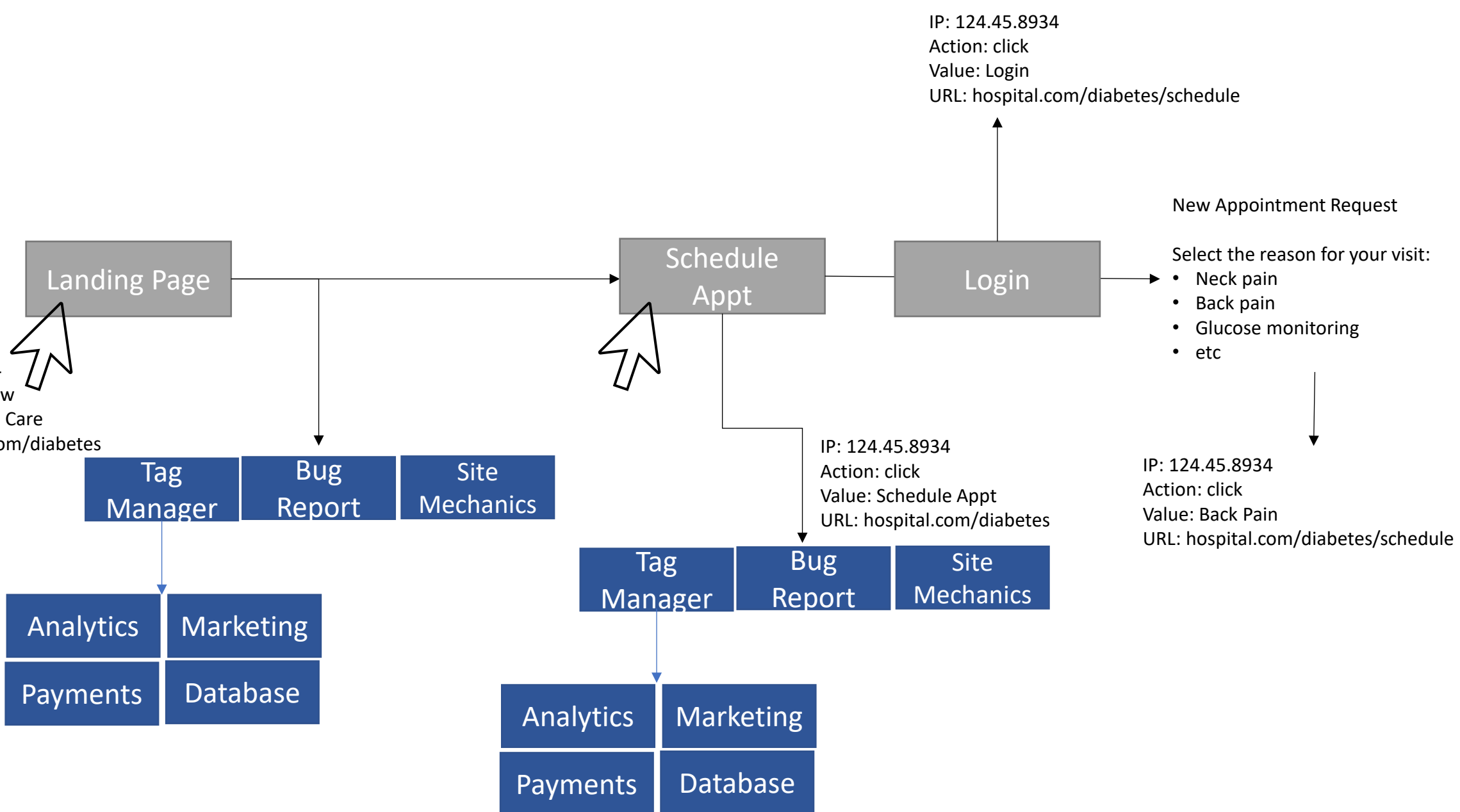
- Using a common lexicon is critical
- Make materials accessible – and therefore usable

# How do I identify and classify my data?



- Bridge the gap between engineering and legal
- Speak the same language – and ask the right questions
- Do some self-learning, and don't be afraid to ask (again and again)
- The responsibility is not just yours





# How do I identify and classify my data?

Adopt a universal, internal definition of sensitive data

Train your workforce (actually)

Know your tech – and empower your people

Build or adopt tools

Classify and control data

- Tools are your friend
- Perfection vs operationalization
- Stay with the market

# How do I identify and classify my data?

Adopt a universal, internal definition of sensitive data

Train your workforce (actually)

Know your tech – and empower your people

Build or adopt tools

Classify and control data

- Technical vs operational controls
- People are the last line of defense

# How do I identify and classify my data?

Adopt a universal, internal definition of sensitive data

Train your workforce (actually)

Know your tech – and empower your people

Build or adopt tools

Classify and control data

# When do I need to obtain consent?

Virginia: A controller shall not process sensitive data concerning a consumer without obtaining the consumer's consent

But: Nothing in this chapter shall be construed to restrict a controller's or processor's ability to provide a product or service specifically requested by a consumer

Washington: A regulated entity or a small business may not collect any consumer health data except: (i) With consent from the consumer for such collection for a specified purpose; or (ii) To the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business.

FTC: Consent required for disclosure of sensitive data?

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

- Do vendors define sensitive data the same way you do?
- Disclosure vs use?

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

- Take a position – and be clear about your risk tolerance
- Is something “necessary” in one state, but not in the other?



# When do I need to obtain consent?

Consider vendor requirements

Define necessary for service vs not

Reference sensitive data classification

Decide between universal approach vs state specific

Exclude certain data wholesale?

- Account for all sensitive data
- Make sure all data elements are tied to a consent (or otherwise “necessary” for service)

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

- Operational simplicity vs potential business loss
- Should some states be excluded wholesale for certain functions?

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

- Certain data may just be untouchable for a given purpose (e.g., authorizations for marketing)

# When do I need to obtain consent?

Consider  
vendor  
requirements

Define  
necessary for  
service vs not

Reference  
sensitive data  
classification

Decide  
between  
universal  
approach vs  
state specific

Exclude certain  
data wholesale?

# How do I obtain consent?

Virginia: "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.

Washington: "Consent" means a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means.

(b) "Consent" may not be obtained by:

- (i) A consumer's acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information;
- (ii) A consumer hovering over, muting, pausing, or closing a given piece of content; or
- (iii) A consumer's agreement obtained through the use of deceptive designs.

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

- What's legally defensible, and what works best for the business?
- Registration flow vs pop-up?

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

- Collect now for necessary purpose and ask for consent later? Or ask now?
- What is the business need (e.g., marketing vs research)



# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

- How broad can a consent be?
- Consider fatigue vs opportunity vs defensibility

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

- Make sure a consent does what it says it does
- What is collection behavior prior to acceptance? If ignored?

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

- If you opt-in, don't forget the opt-out – and how that is operationalized

# How do I obtain consent?

Consider your interactions with customer

Consider anticipated uses, and when use will be made

What is the scope of consent?

Monitor behavior of banners (if used)

Provide opt-out option

# Unfortunately, no approach is universal.

- Limit use of sensitive information
- Maryland prohibition on use
- ... and whatever else is coming down the pipeline.

Thank you!