Navigating the Intersection of Health Data, AI, and Privacy Law: Current Trends and Legal Implications

We're all connected.

LOEB & LOEB LLP

LOS ANGELES
NEW YORK
CHICAGO
NASHVILLE
WASHINGTON, DC
SAN FRANCISCO
BEIJING
HONG KONG

loeb.com

Speakers

Jessica B. Lee
Chair, Privacy, Security & Data Innovations
Loeb & Loeb LLP

John Hegeman
Senior Associate General Counsel
Optum

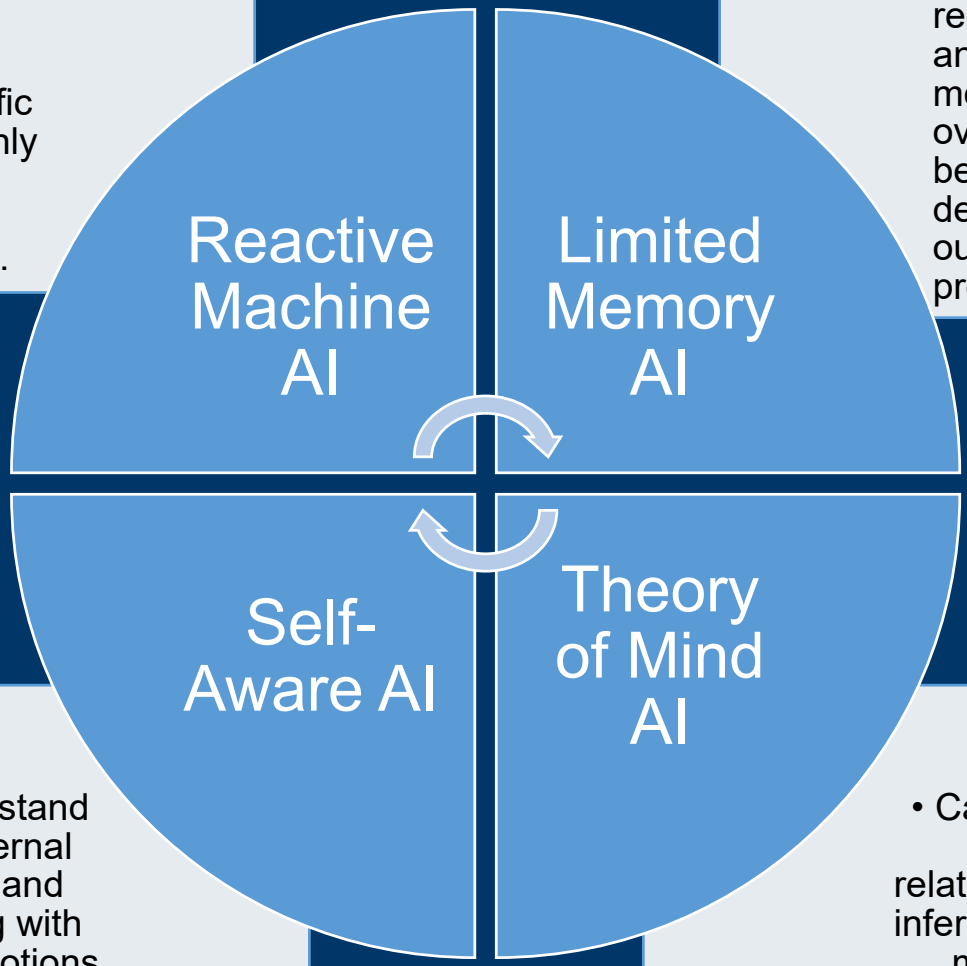
Eric Cook
Attorney, Privacy, Security & Data Innovations
Loeb & Loeb LLP

The opinions expressed in this document do not necessarily reflect the views of Loeb & Loeb LLP or its clients. This document was created for purposes of teaching and commentary, and should not be posted to the Internet, or otherwise used for any commercial purposes, without prior written approval from Loeb & Loeb LLP. The information in this document is not intended to be and should not be taken as legal advice.

Today's Agenda

- Level-Setting: What is AI?
- Understanding the Use Cases: What are the Practical Applications of AI in Healthcare?
- Key Issues—Throughout the Lifecycle
  - Design
  - Develop
  - Deploy
  - Review
- Building a Review Cycle for Privacy and Ethical Data
  - Bias, Fairness, transparency, and mitigating discrimination

WHAT IS AI?



Recommendation Engines

- AI systems with no memory designed to perform specific tasks. They only work with presently available data.

- AI systems that can recall past events and outcomes and monitor situations over time. Data can be used to determine the best outcome for a problem/query.

Generative AI, Chatbots, Self-Driving Cars

Does not exist today!

- Can understand its own internal conditions and traits along with human emotions and thoughts.

- Can simulate human-like relationships by inferring human motives and reasoning.

Does not exist today!

The Healthcare Industry is an Early Adopter of AI Systems

- Disease Identification and Diagnosis
- Personalized Medicine
- Drug Discovery and Development
- Clinical Trial Research
- Virtual Health Assistants and Chatbots
- Health Monitoring and Wearables
- Predictive Analytics
- Epidemiology and Disease Surveillance

Virtua Health is bringing on AI therapists amid provider shortage

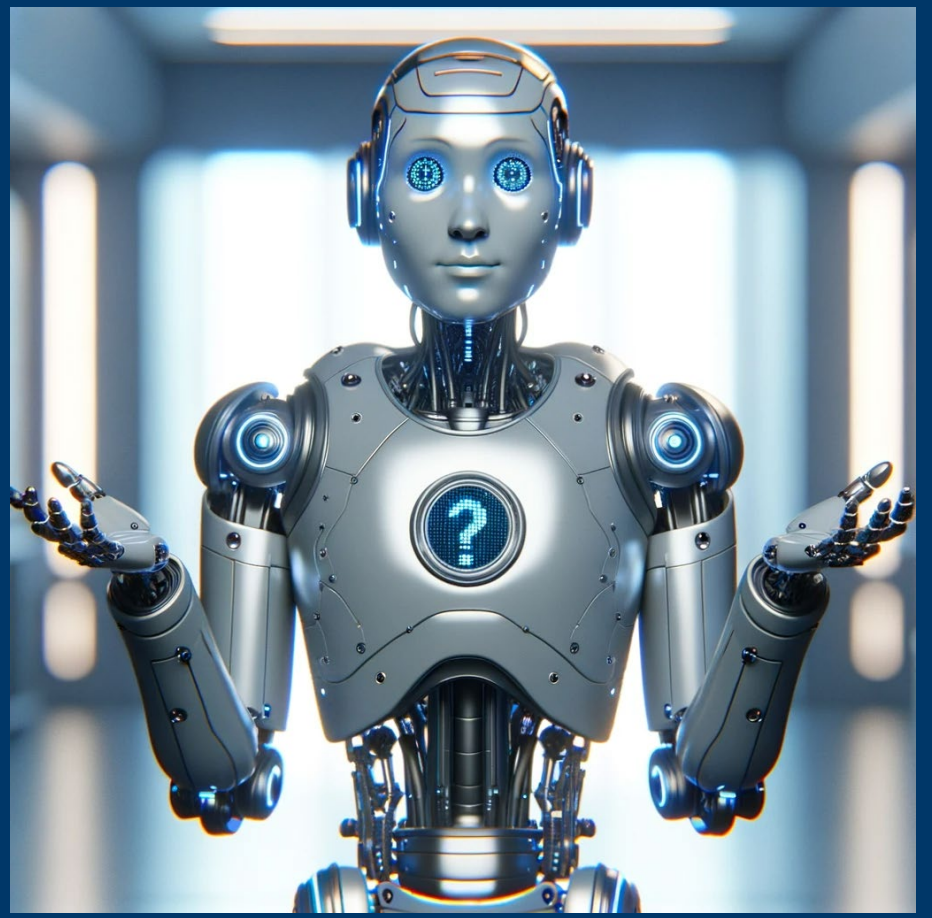
Cognosos Leverages AI to Make Smart Real-Time Location Services Accurate and Affordable

Emory Healthcare to Pilot AI-Powered Virtual Inpatient Monitoring

Doctors Wrestle With A.I. in Patient Care, Citing Lax Oversight

The F.D.A. has approved many new programs that use artificial intelligence, but doctors are skeptical that the tools really improve care or are backed by solid research.

WHAT COULD GO WRONG?



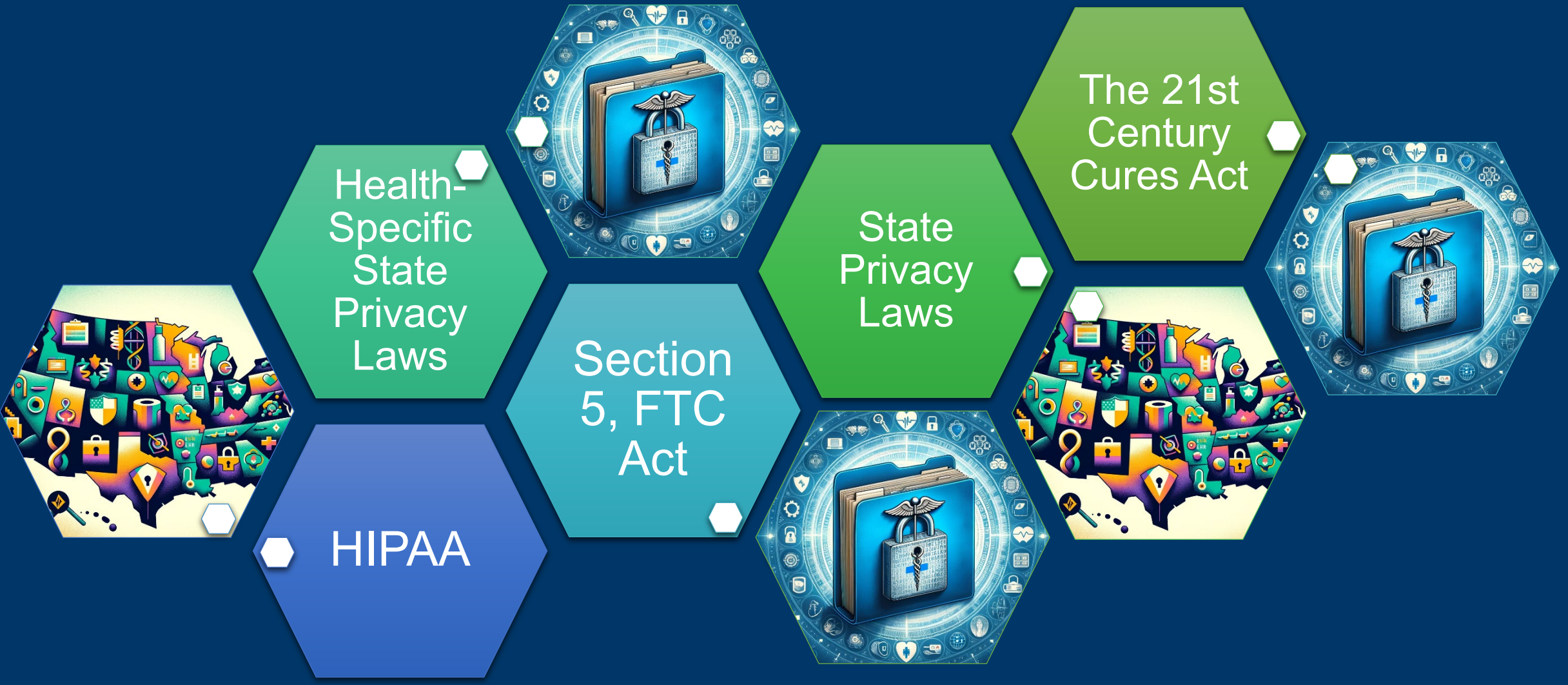
What happens when an algorithm cuts your health care

“The Framingham Heart Study cardiovascular risk score performed very well for Caucasian but not African American patients, which means that care could be unequally distributed and inaccurate. In the field of genomics and genetics, it’s estimated that Caucasians make up about 80 percent of collected data, and thus studies may be more applicable for that group than for other, underrepresented groups.”

WHAT DO COMPANIES IN THIS SPACE NEED TO HELP NAVIGATE THE CHALLENGES ?

Understanding the Legal Landscape

What Laws Govern?



DOES HIPAA APPLY?

Are you a Covered Entity?

- Healthcare Providers
- Health Plans
- Health Clearinghouses

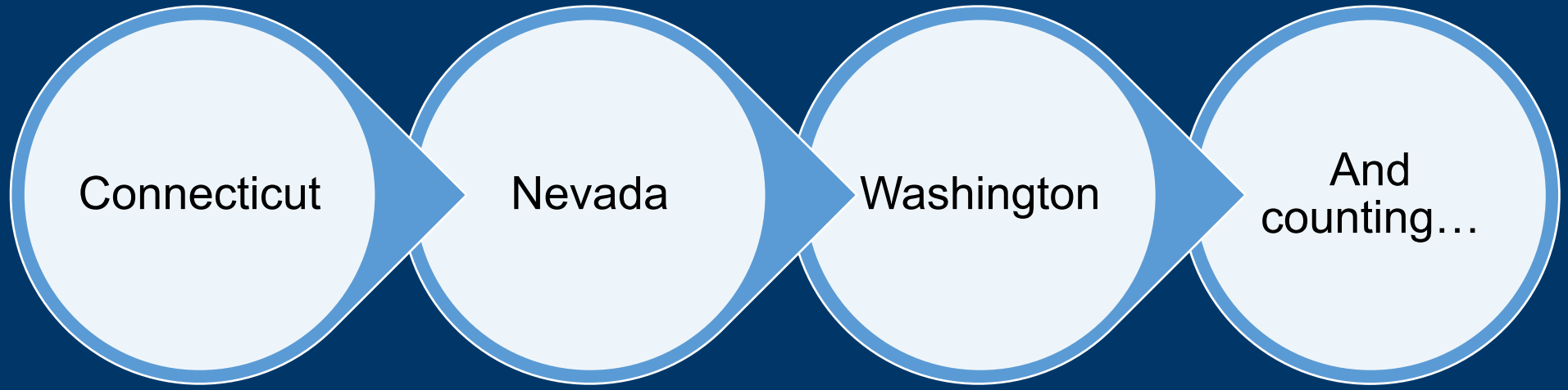
Are you a Business Associate?

- Creates, receives, maintains, or transmits PHI for HIPAA regulated activity.
- Provides certain services to or for the covered entity.
- Provides data transmission services for a covered entity.

Is the Data PHI? Does it relate to:

- An individual's past, present, or future physical or mental health or condition
- The provision of health care to an individual
- The past, present, or future payment for the provision of health care to an individual

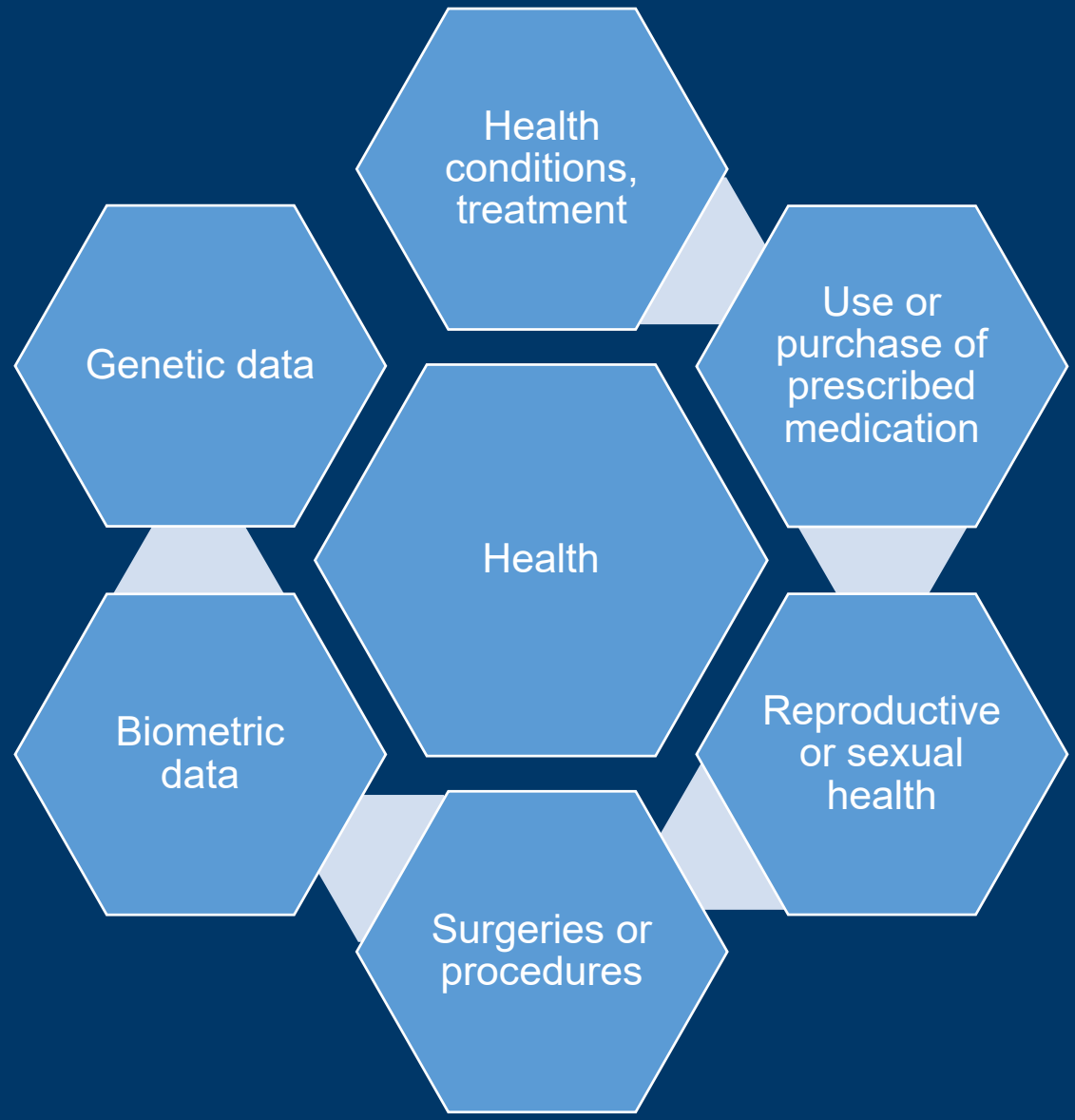
Does a Health-Specific State Privacy Law Apply?



What is Health Data?

Personal information that is:

- linked or reasonably linkable to a consumer
- identifies the consumer's past, present, or future physical or mental health status.



*

What Role will the FTC Play?

Section 5 of the FTC Act.

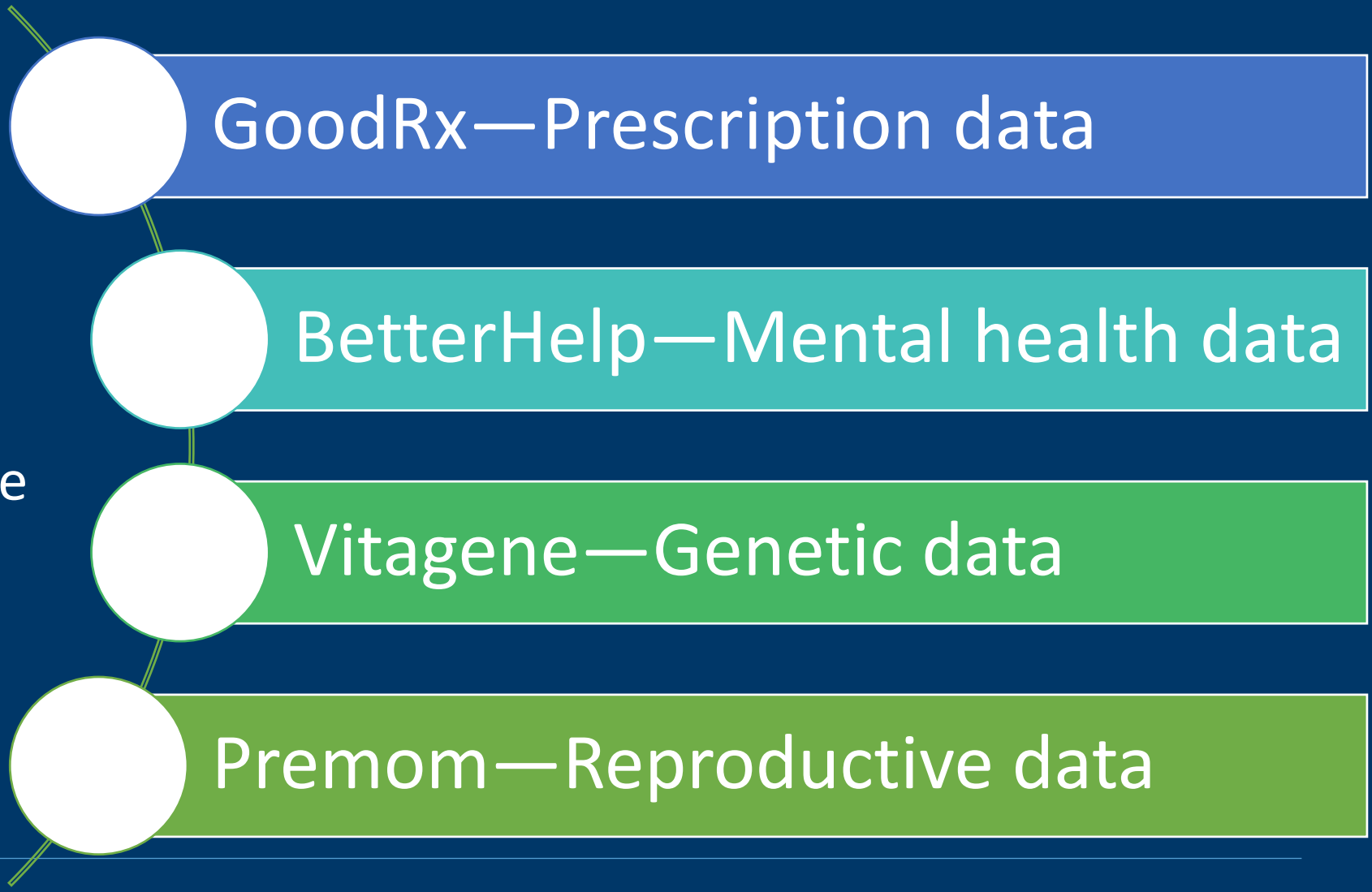
The FTC Act prohibits unfair or deceptive practices. That would include the sale or use of – for example – racially biased algorithms.

Health Breach Notification Rule

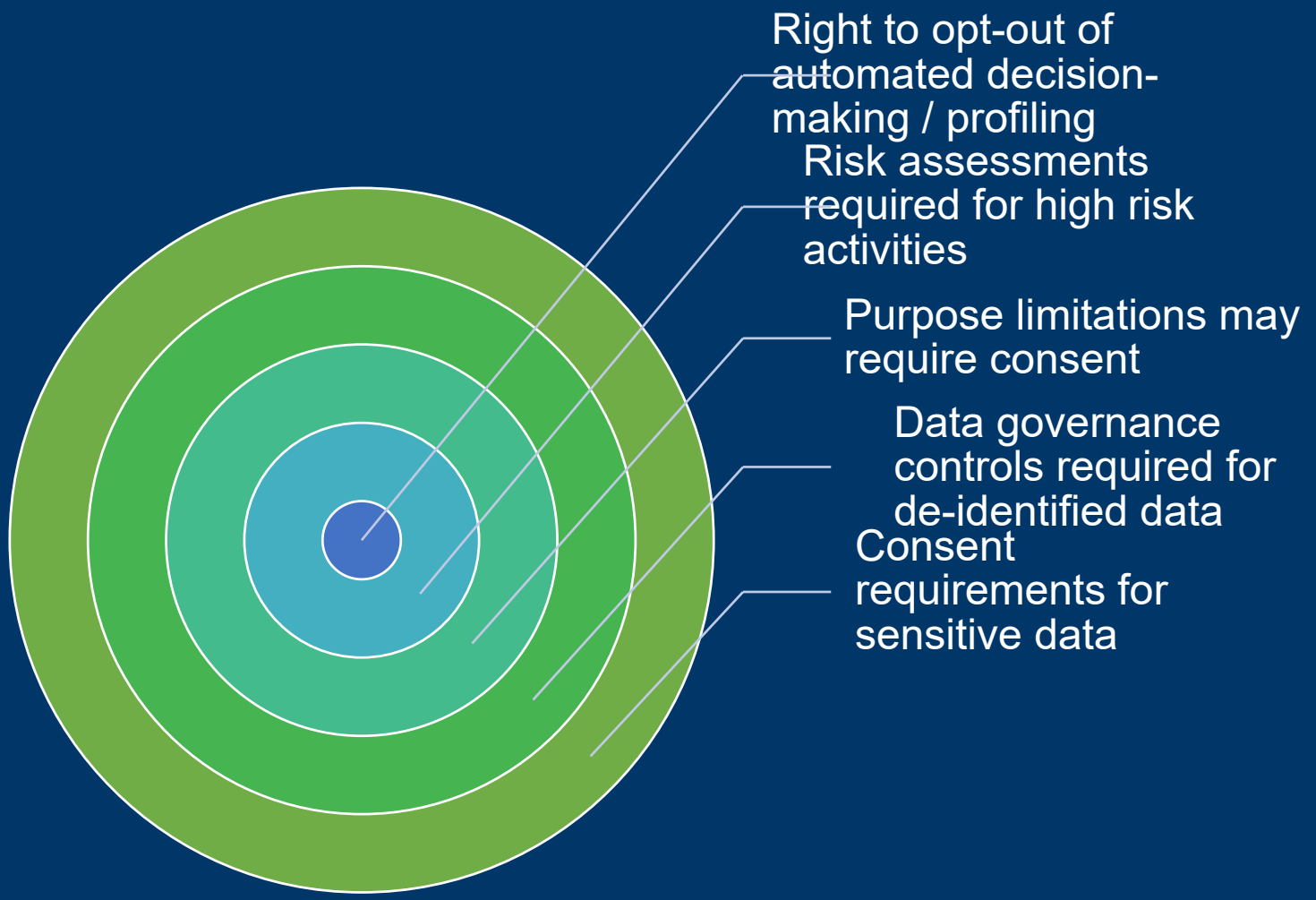
The HBNR comes into play in when health data that is disclosed to a business at a consumer's direction is improperly disclosed to an entity without the consumer's consent.

FTC Definition of Sensitive Personal Information

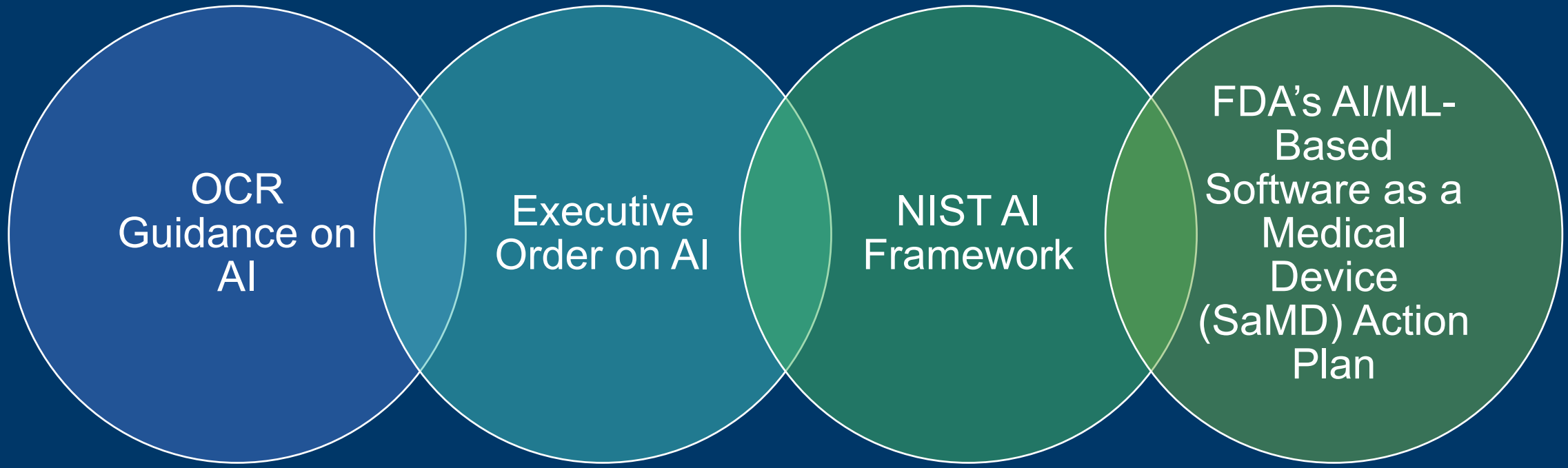
- Any identifiable or reasonably identifiable consumer health information or information that could be used to infer health information about a consumer.



Impact of State Privacy Laws



WHAT REGULATIONS/GUIDANCE SHOULD BE CONSIDERED



NIST AI FRAMEWORK

Risk Management and Assessment:

- Emphasizes the need for a comprehensive AI risk management approach that includes identifying, assessing, managing, and communicating risks associated with AI systems.

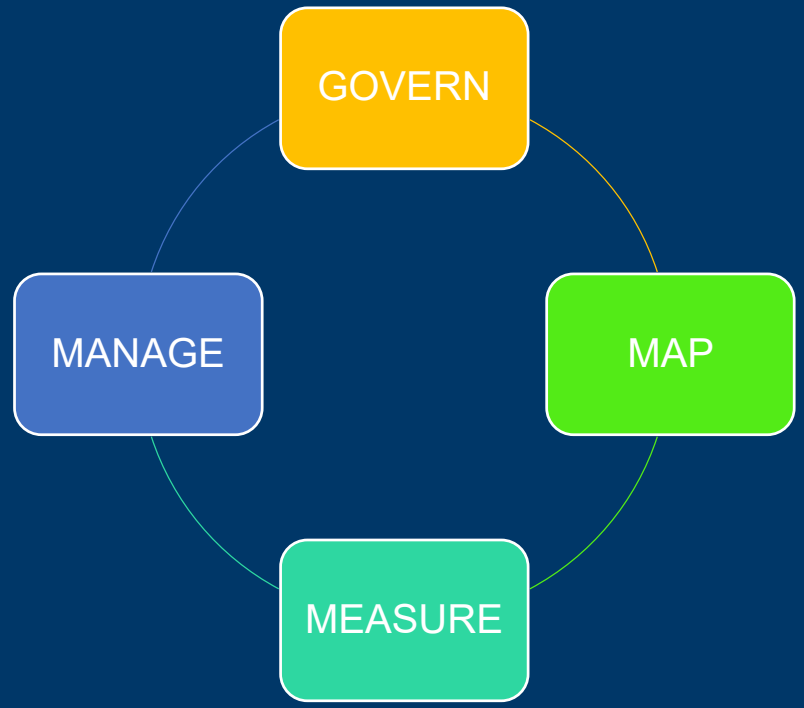
Reliability, Validity, and Safety:

- Calls for ensuring AI systems are reliable and valid for their intended use, and that they are safely integrated into operational processes without unintended consequences.

Transparency and Explainability:

- Stresses the importance of transparency in AI processes and decision-making, ensuring that AI actions are explainable to stakeholders in a clear and understandable manner.

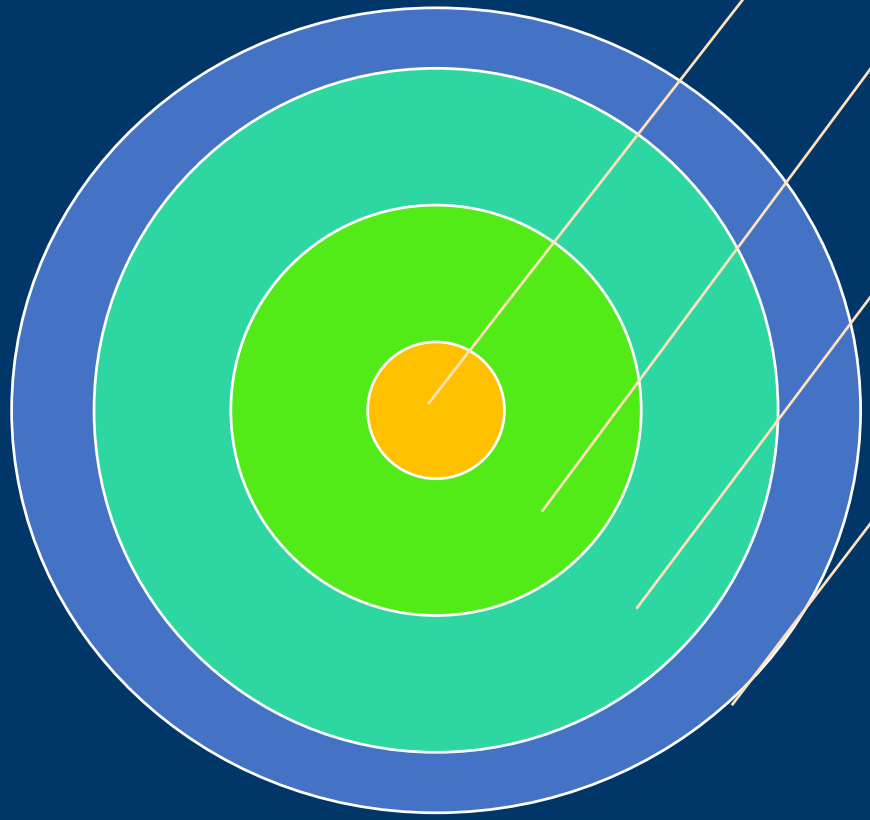
4 FUNCTIONS TO ADDRESS RISK



Biden's Executive Order

- Existing consumer protection laws will enforced, including:
  - Nondiscrimination
  - Privacy
  - Security
  - Fraud
- HHS AI Task Force will be charged with creating policies and frameworks concerning responsible deployment of AI technologies in research, discovery, drug and device safety, healthcare delivery and financing as well as public health, including
  - Human Oversight
  - Mitigating Discrimination and Bias
  - Safety, Privacy, and Security in Software-development lifecycle

OCR GUIDANCE ON AI



AI systems should be designed to maintain the public trust

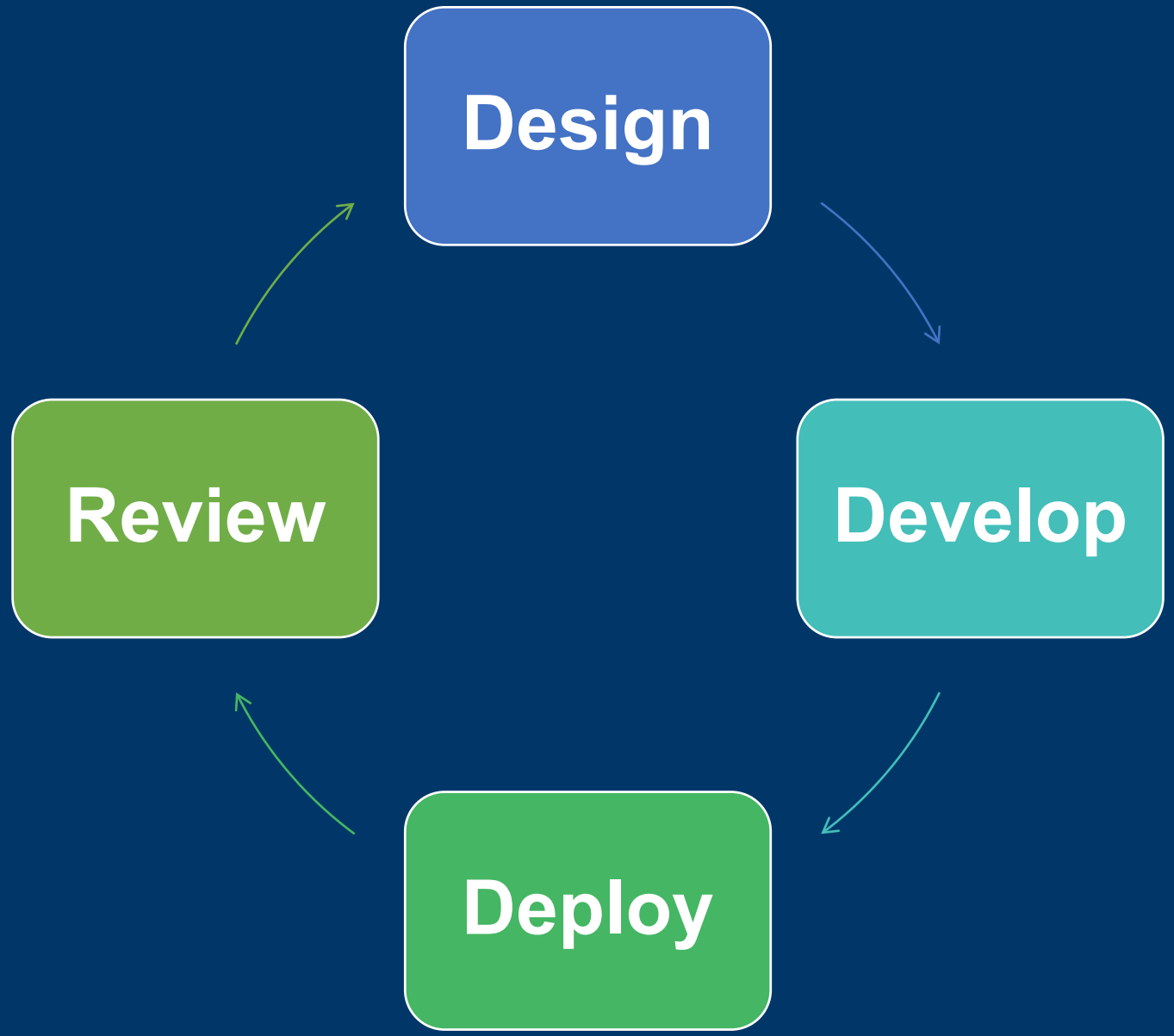
Trustworthy AI requires the design, development, and acquisition of AI to be considered in the context of privacy, civil right, and civil liberties.

Governed by EO 13960, “Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government”

AI Lifecycle that aligns with HHS
Enterprise framework, includes: initiation and concept, research and design, develop, train, and deploy, and finally operate and maintain.

Let’s Apply this to the Review Lifecycle

AI Review Cycle

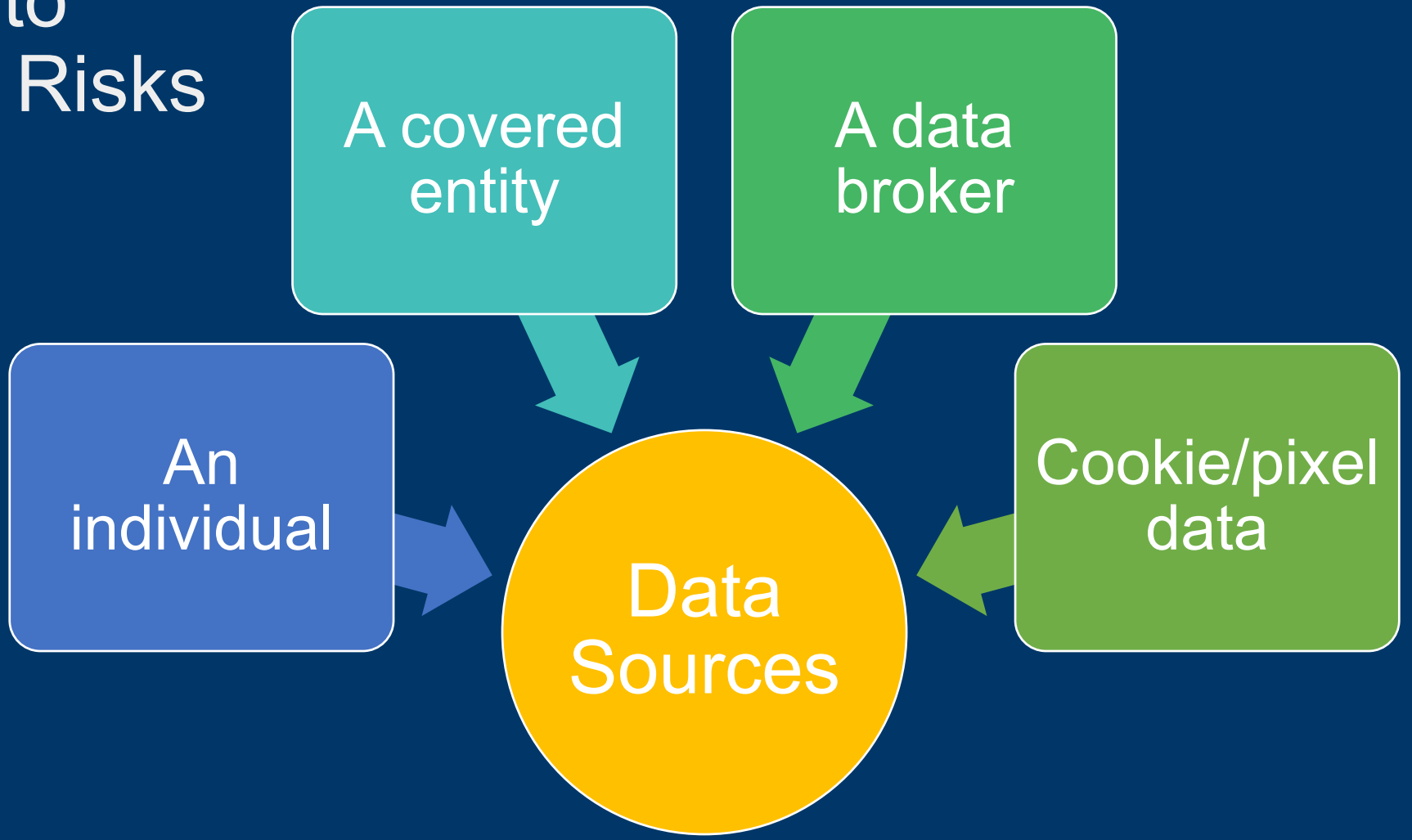


DESIGN

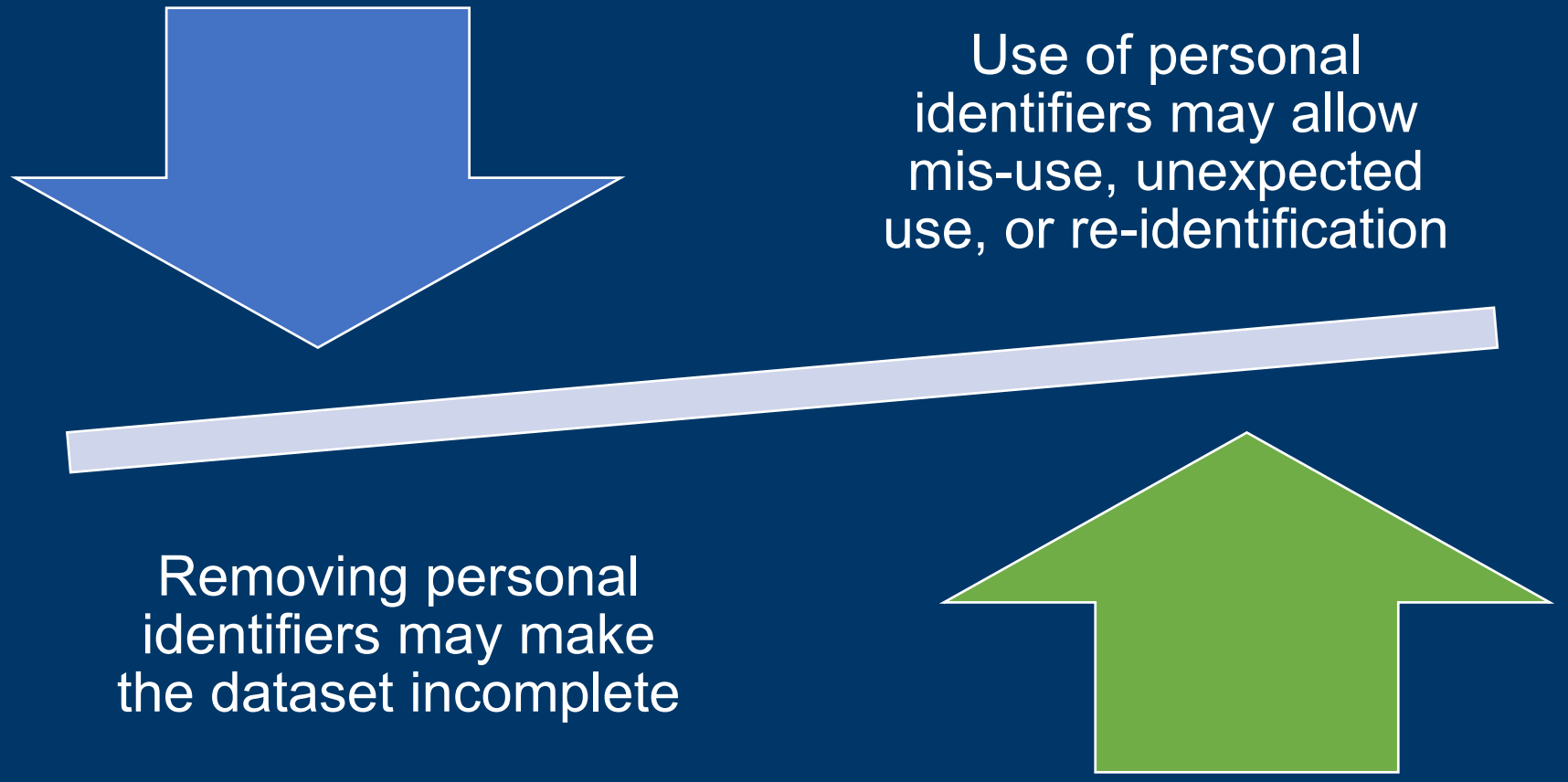
KEY QUESTIONS:

- WHAT IS THE USE CASE?
- WHERE DO WE SEE THE ROI?
- WHAT COULD GO WRONG?

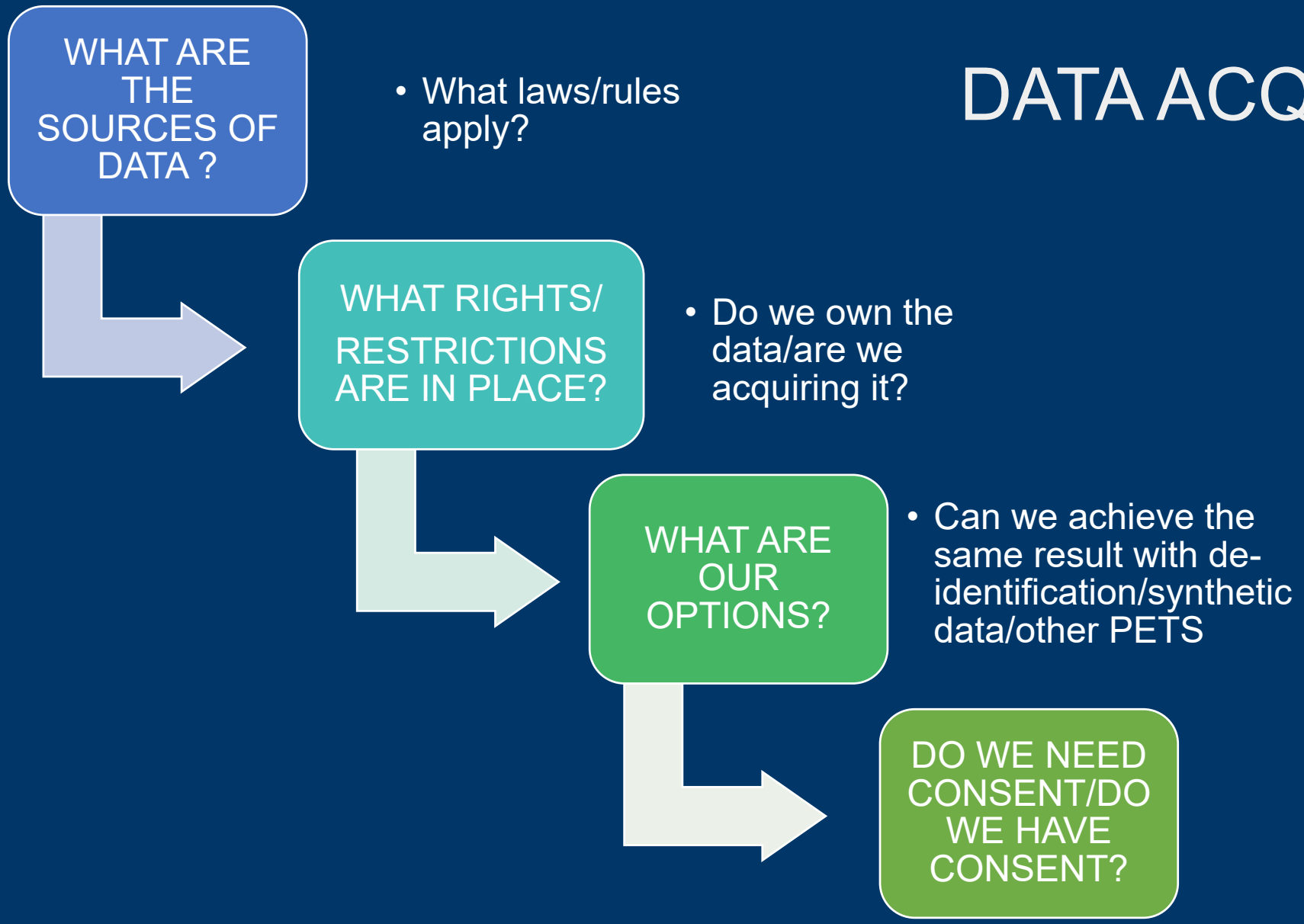
Understand the Source of Data to Understand the Risks and Obligations



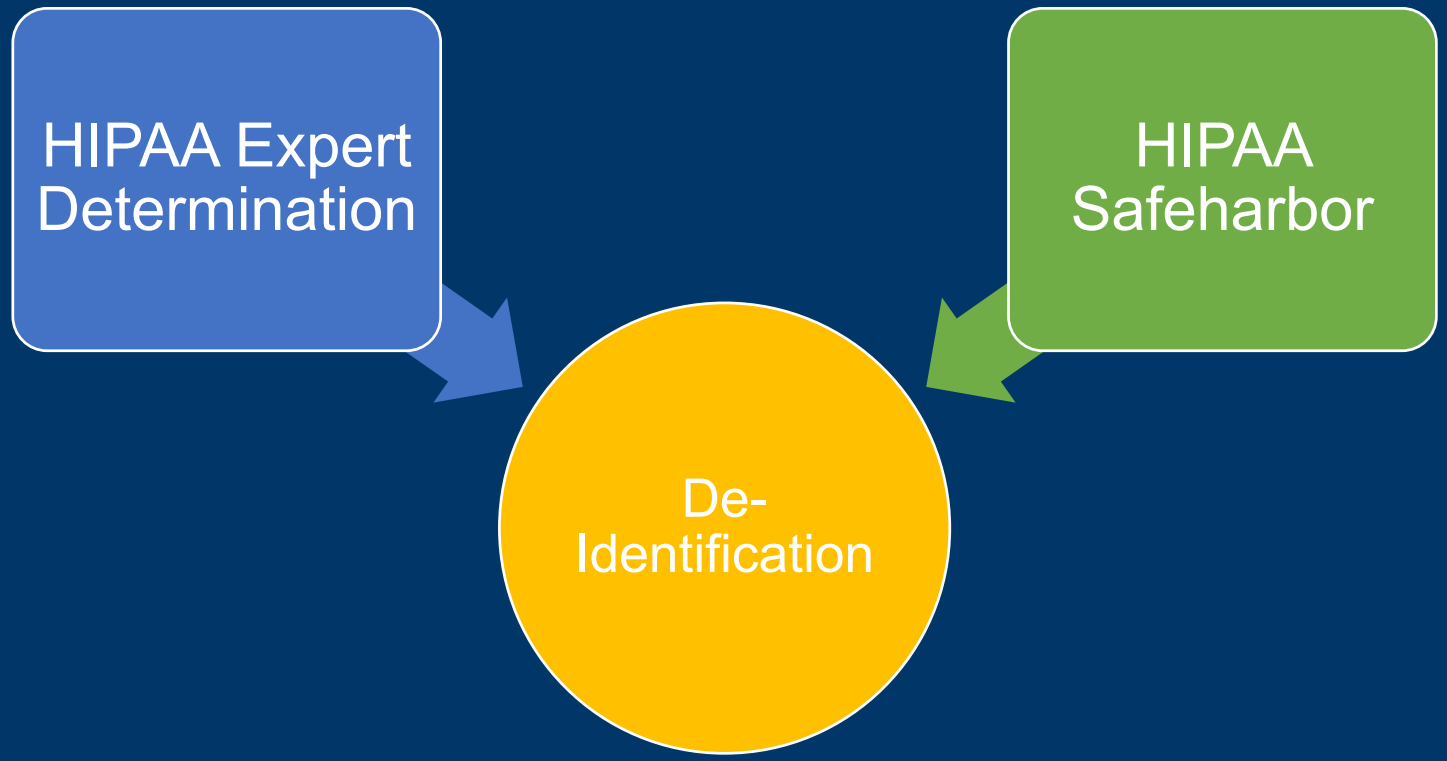
Personal Information in AI Systems



DATA ACQUISITION



HIPAA Deidentification

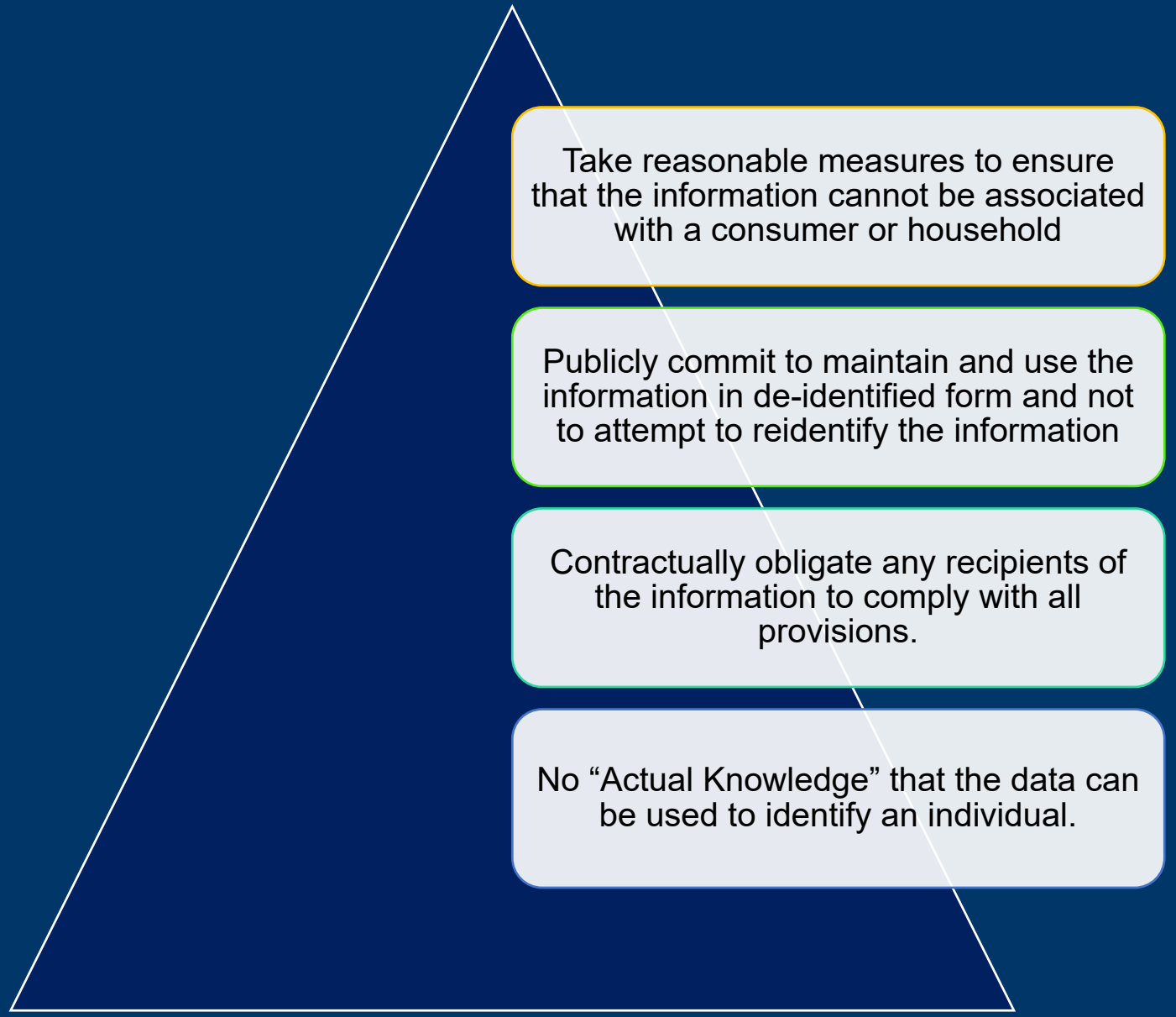


18 Identifiers to Remove for De-Identification:

- Names (Full or last name and initial)
- All geographical identifiers smaller than a state*
- Dates (other than year) directly related to an individual
- Phone Numbers
- Fax numbers
- Email addresses
- Social Security numbers
- Medical record numbers
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers (including serial numbers and license plate numbers)
- Device identifiers and serial numbers;
- Web Uniform Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger, retinal and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

*

Additional Governance Controls

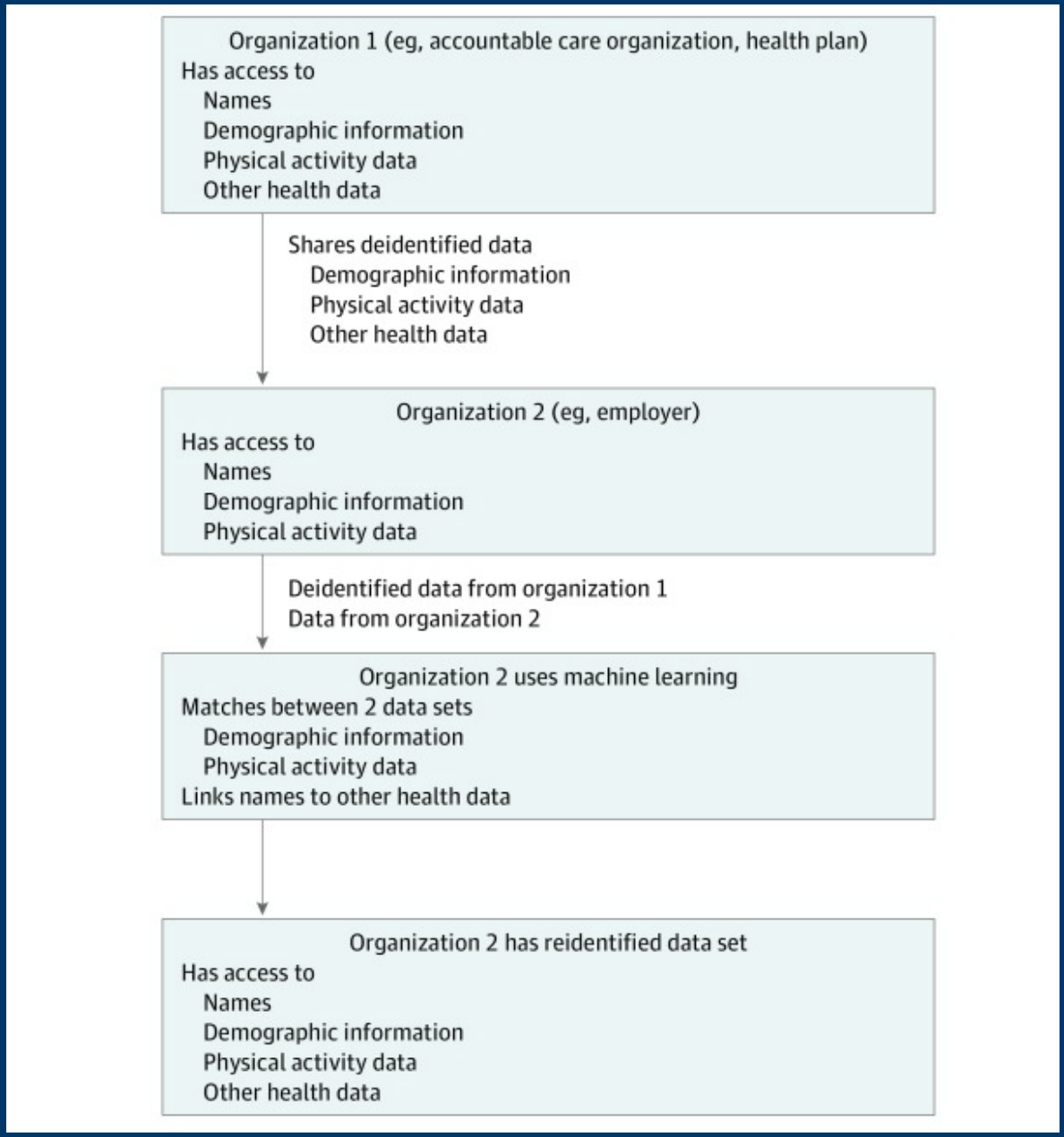


"The de-identification of individual-level data cannot, on its own, protect privacy as it is simply too difficult to prevent re-identification."

32

A Closer Look at Re-Identification

A feasibility study by the JAMA Network used an algorithm to re-identify physical activity data where geographic and PHI data had been removed after being collected from wearables. Indirect identifiers used.



Forms of Consent for Health Data

Opt-in/Opt-out Consent

- California Consumer Privacy Act (CCPA) (Opt-out)
- Colorado Privacy Act (Opt-in)
- Connecticut Privacy Act (Opt-in)
- Utah Privacy Act (Opt-out)
- Virginia data Protection Act (Opt-in)

Signed Written Authorization

- HIPAA
- Clinical Research
- Washington's My Health My Data Act (MHMD) when disclosure qualifies as a "sale" of data

Obtaining Consent

(Opt-in vs. Opt-out)

- Affirmative Act
- Freely given
- Specific
- Informed

Written Authorization

- Description of the data, use, and what the data is being disclosed for.
- Revocation right
- Notice the data may no longer be protected if redisclosed to a third party and that treatment is not conditioned on the signing of the authorization
- Revocation right
- Signed and Dated

BACK TO THE USE CASE –

WHAT RULES IMPACT THE USE CASE?

IS A HUMAN IN THE LOOP?

WILL YOU BE ABLE TO EXPLAIN HOW THE OUTCOMES ARE REACHED?

Ethical Considerations for Bias and Discrimination

Does this data use case treat individuals differently based on their protected class or treat at-risk individuals differently based on their status?

Will this data use have the impact of treating individual differently based on their protected class?

Is this data use case likely to cause the provision or denial of health care services?

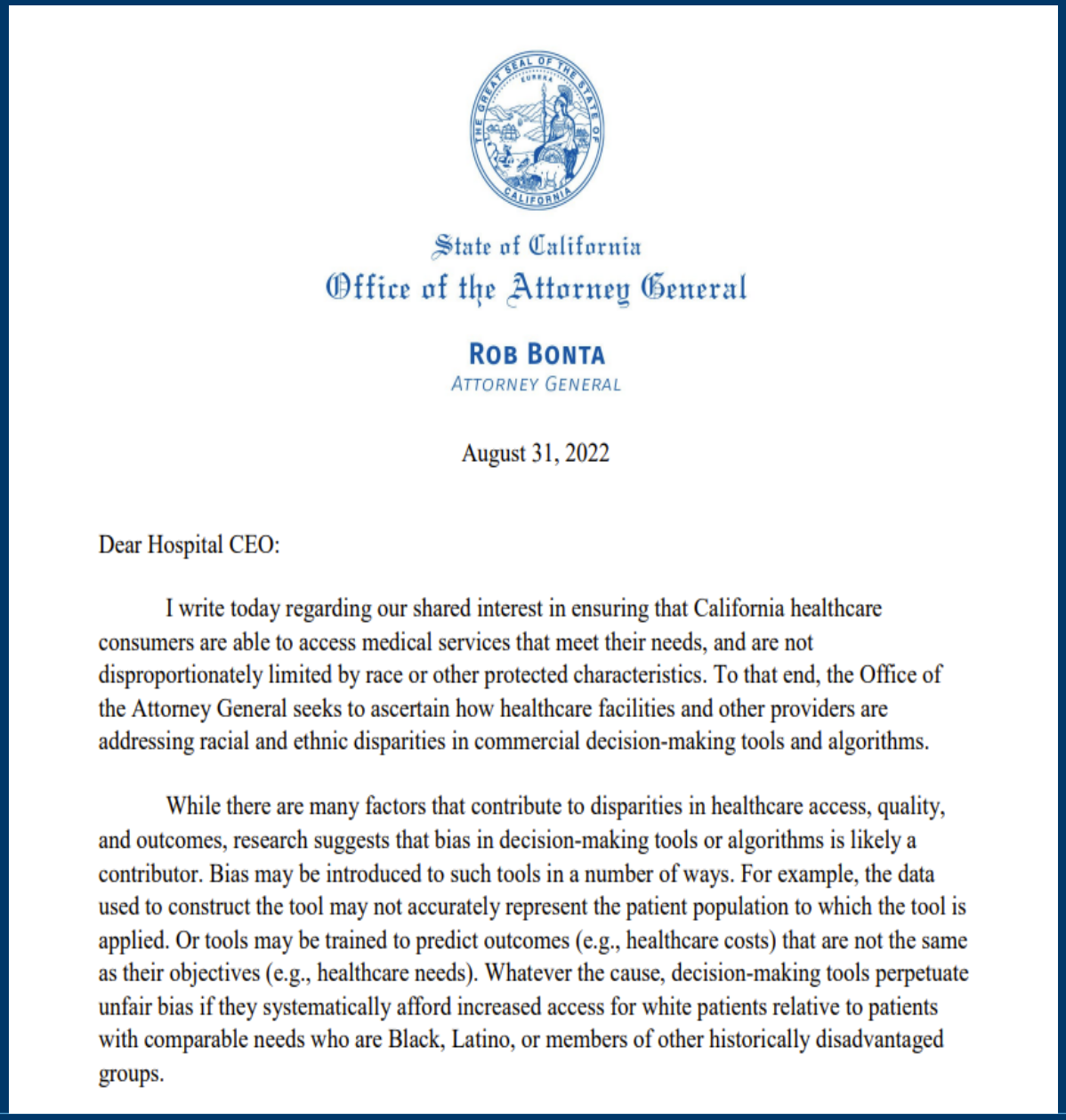
Key Takeaway: Bias and discrimination are often automatic and unconscious processes that we must deliberately test for in the data before and after it is used.

Understanding the Risk for Bias

- Superficially ‘neutral’ AI can produce and reinforce discrimination on the basis of protected characteristics like race, religion, or sex.
- If a data set is missing information from particular populations, using that data to build an AI model may yield results that are unfair or inequitable to legally protected groups.
- Health care AI tools can also use data that inadvertently captures systemic racism, adding to existing inequities in health care access and status.

*

In August 2022, CA AG Rob Bonta issued a letter to hospitals requesting information about all commercially available or purchased decision-making tools, products, software systems, or algorithmic methodologies in use at hospitals, flagging the risk of bias.



State of California
Office of the Attorney General

ROB BONTA
ATTORNEY GENERAL

August 31, 2022

Dear Hospital CEO:

I write today regarding our shared interest in ensuring that California healthcare consumers are able to access medical services that meet their needs, and are not disproportionately limited by race or other protected characteristics. To that end, the Office of the Attorney General seeks to ascertain how healthcare facilities and other providers are addressing racial and ethnic disparities in commercial decision-making tools and algorithms.

While there are many factors that contribute to disparities in healthcare access, quality, and outcomes, research suggests that bias in decision-making tools or algorithms is likely a contributor. Bias may be introduced to such tools in a number of ways. For example, the data used to construct the tool may not accurately represent the patient population to which the tool is applied. Or tools may be trained to predict outcomes (e.g., healthcare costs) that are not the same as their objectives (e.g., healthcare needs). Whatever the cause, decision-making tools perpetuate unfair bias if they systematically afford increased access for white patients relative to patients with comparable needs who are Black, Latino, or members of other historically disadvantaged groups.

What Questions Should We Ask to Mitigate Bias?

How big and representative is the training database?

What is the source of the data?

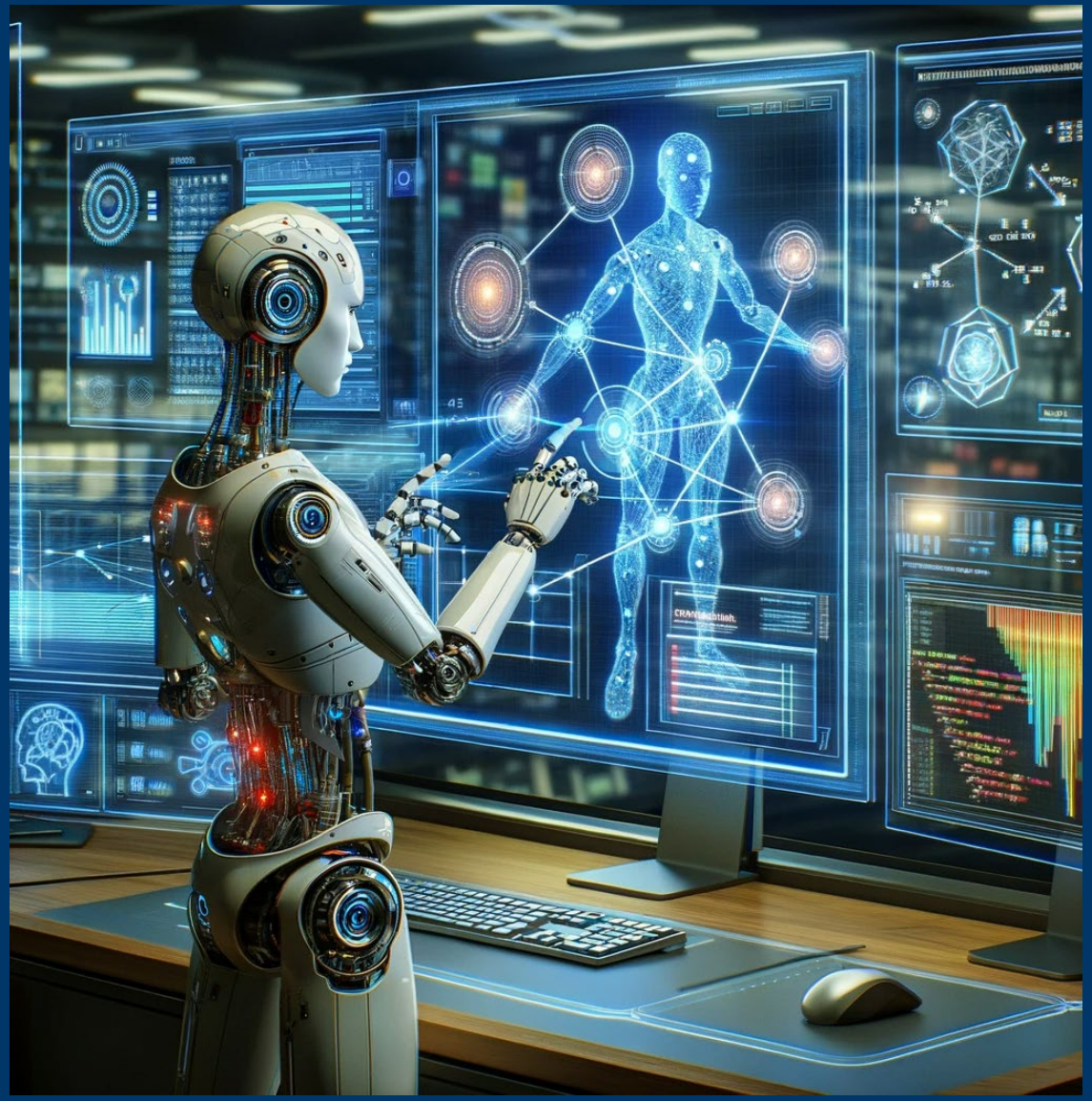
How were the data sets labeled?

What type of quality controls are in place to govern the tagging process?

How diverse is the team developing the algorithms?

Do the Outcomes Match the Objectives?

WHAT OTHER QUESTIONS ARE YOU ASKING?



DEVELOP (AND TEST!)

KEY QUESTIONS?

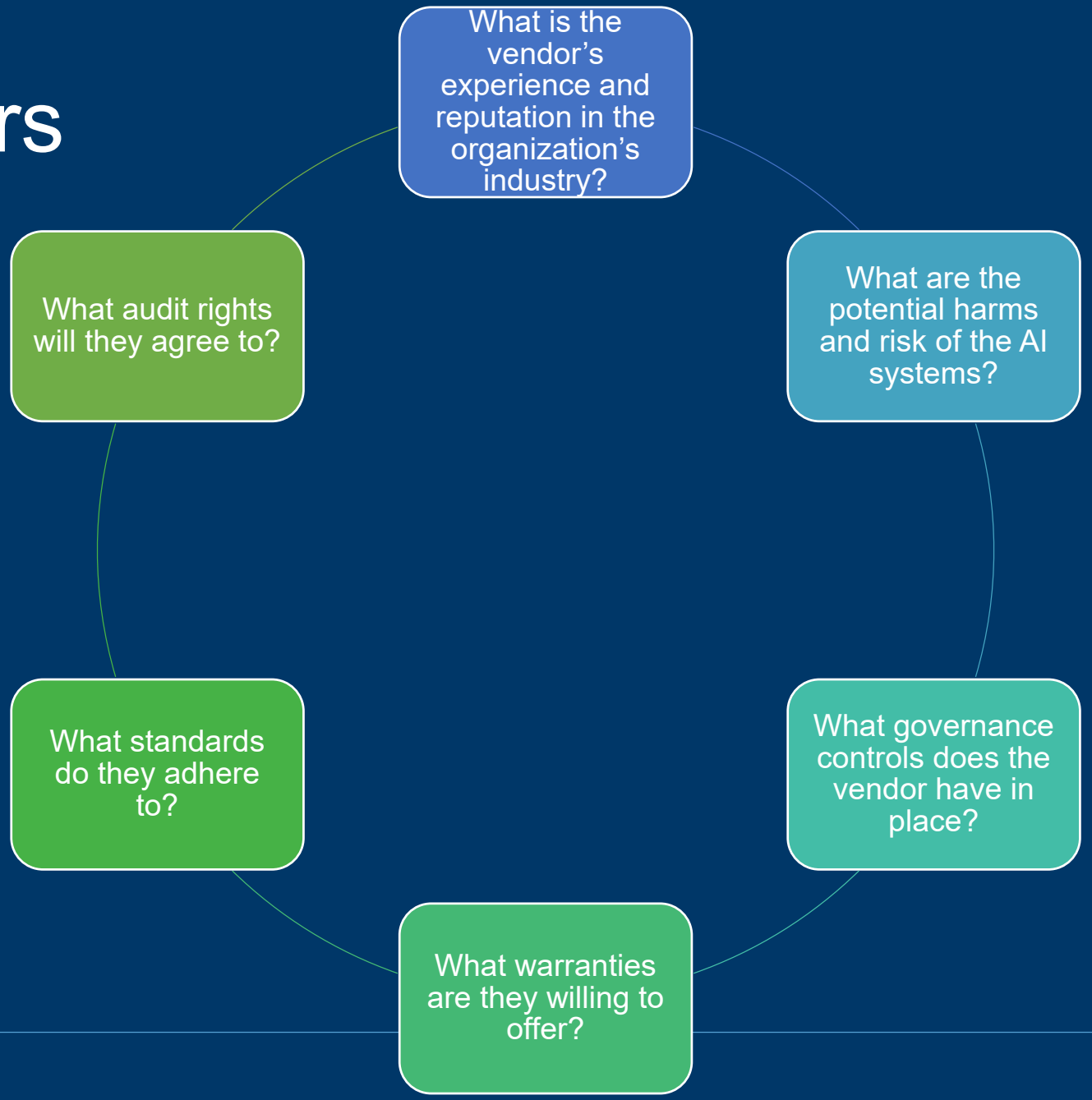
IS DEVELOPMENT INTERNAL OR VIA A THIRD PARTY?

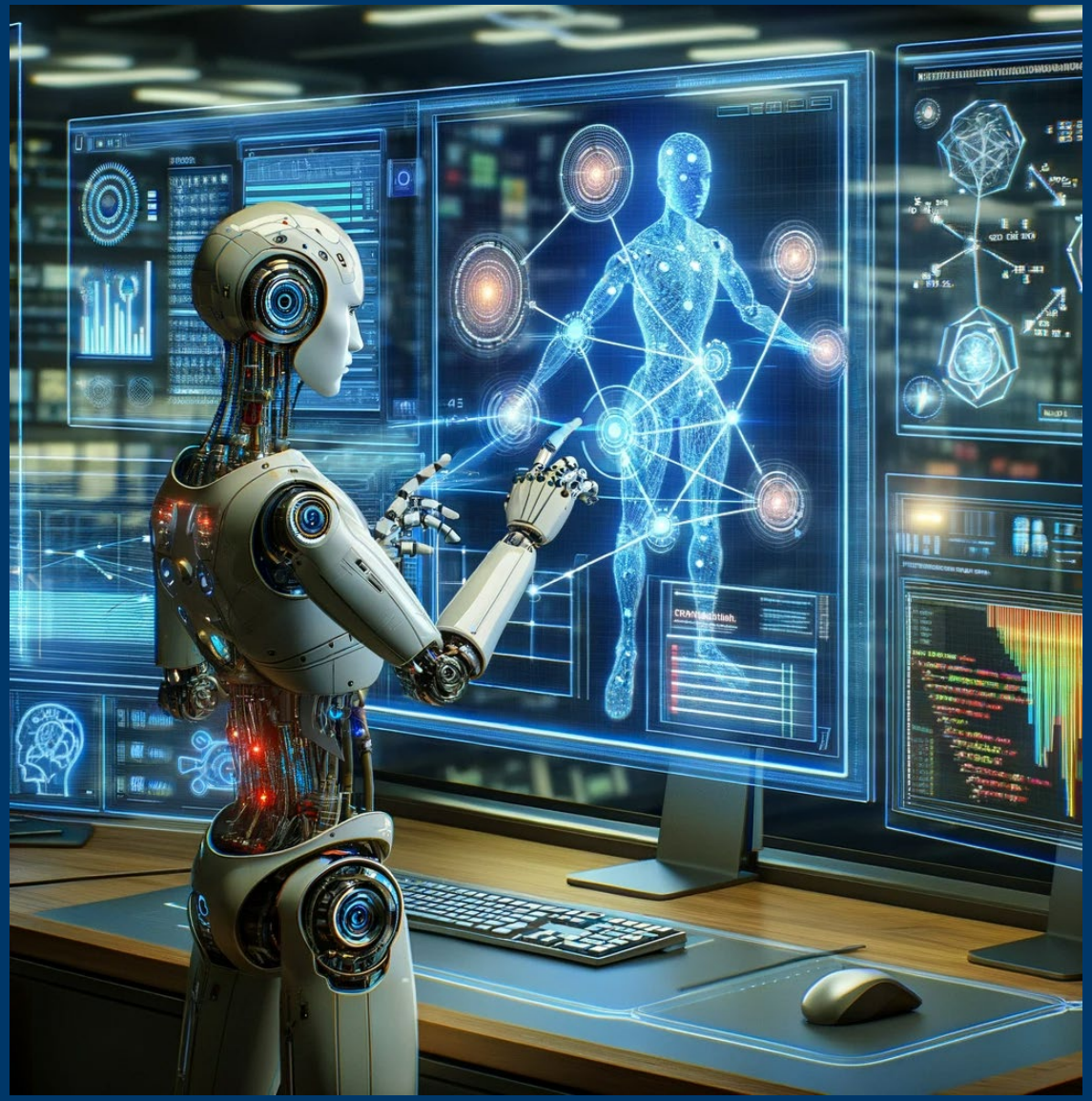
HOW IS LIABILITY/RESPONSIBILITY ALLOCATED?

WHAT ARE THE LIMITATIONS OF THE DATA SET AND HOW TO CORRECT FOR THEM?

HOW TO DESIGN AN ALGORITHMIC ASSESSMENT?

Vetting Your Vendors



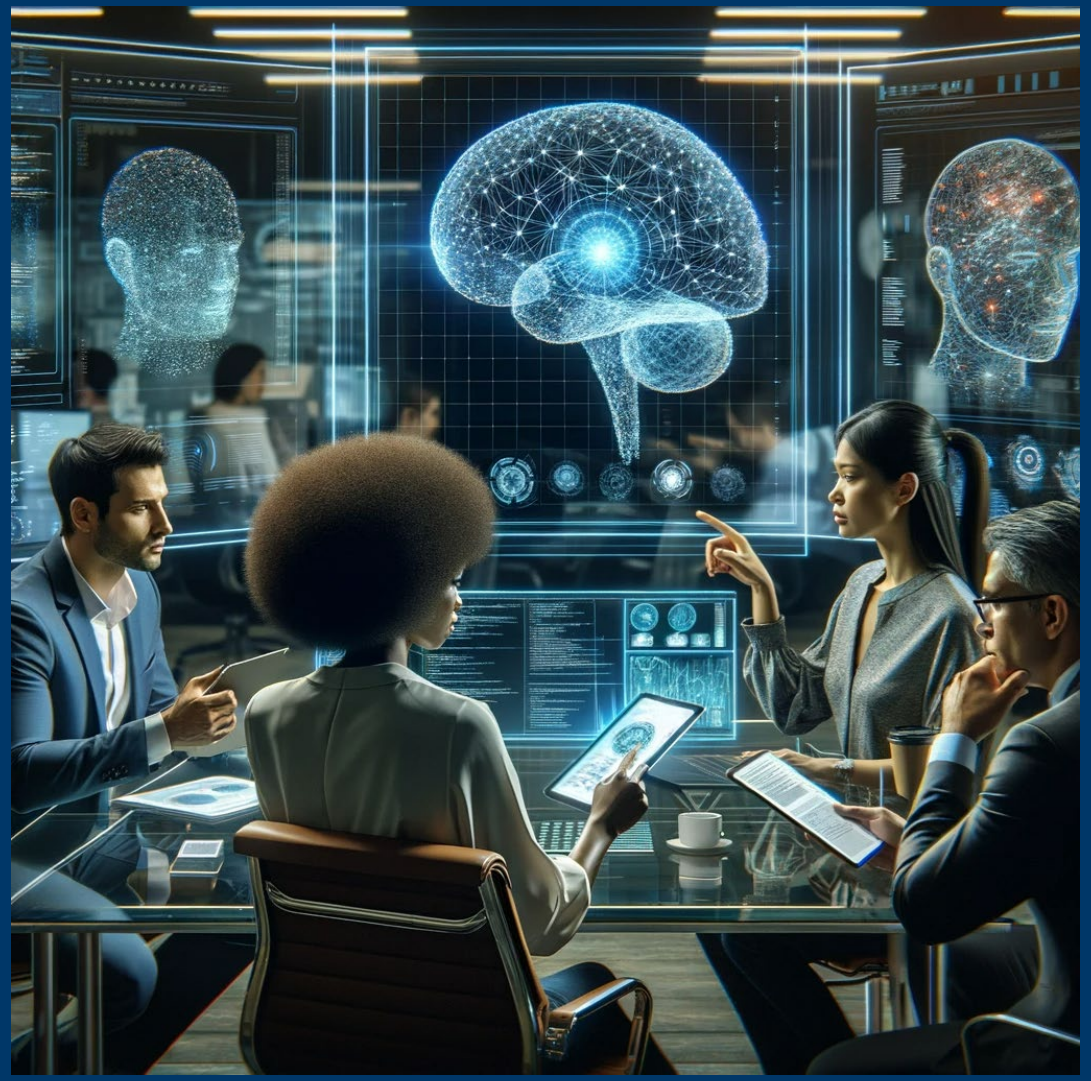


DEPLOY

Incorporate Consumer Rights

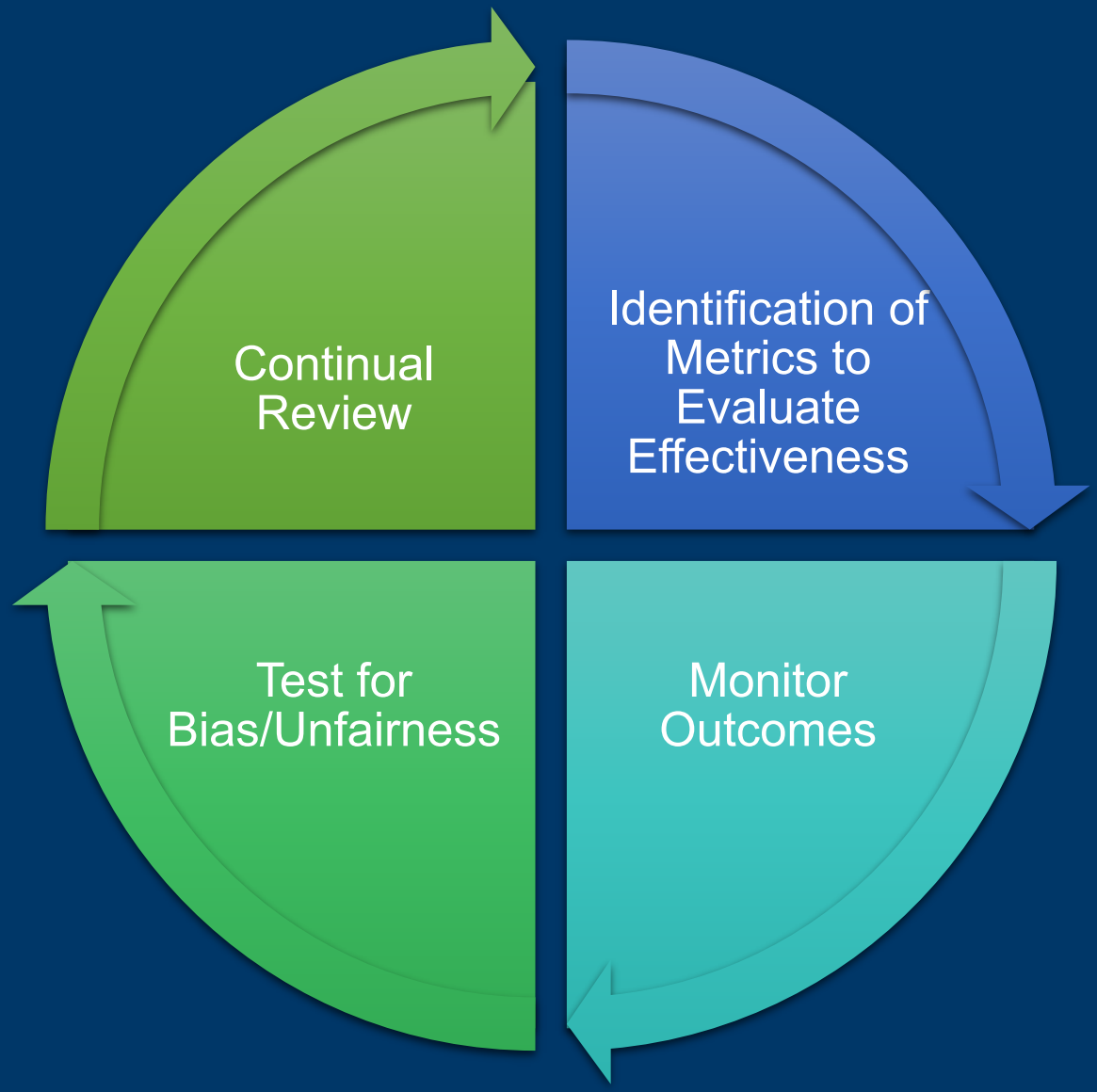
- Incorporating consumer and data subject rights to increase transparency
- Right to correct
  Right to delete
  Right to opt-out
  Right to human intervention
- Use of consumer rights to detect and correct issues with AI systems

WHAT OTHER QUESTION DO YOU ASK IN THE DEPLOYMENT PHASE?



REVIEW

REVIEWING AND AUDITING



HOW DO YOU AUDIT/ASSESS YOUR AI SYSTEMS?

WRAPPING UP

*

CREATE A CROSS-FUNCTIONAL TEAM

IT	Legal	Data Scientists	Employment
Security	Marketing	HR	Intellectual Property

Key Activities for AI Governance

- DEVELOP POLICIES AND PROCEDURES TO OPERATIONALIZE AI SYSTEM MANAGEMENT
- CREATE A CADENCE FOR REGULAR REVIEW OF SOFTWARE CODES, AND POLICIES
- ALIGN EXTERNAL STATEMENTS WITH INTERNAL PRACTICES

What Questions Should You Be Asking?

What are we using our AI system for?

Who is the intended audience?

Which laws apply (e.g., EU, FTC, California, New York)?

What are our data sources?

Who are the vendors and what assurances do they provide?

Who are the individuals whose information will be used?

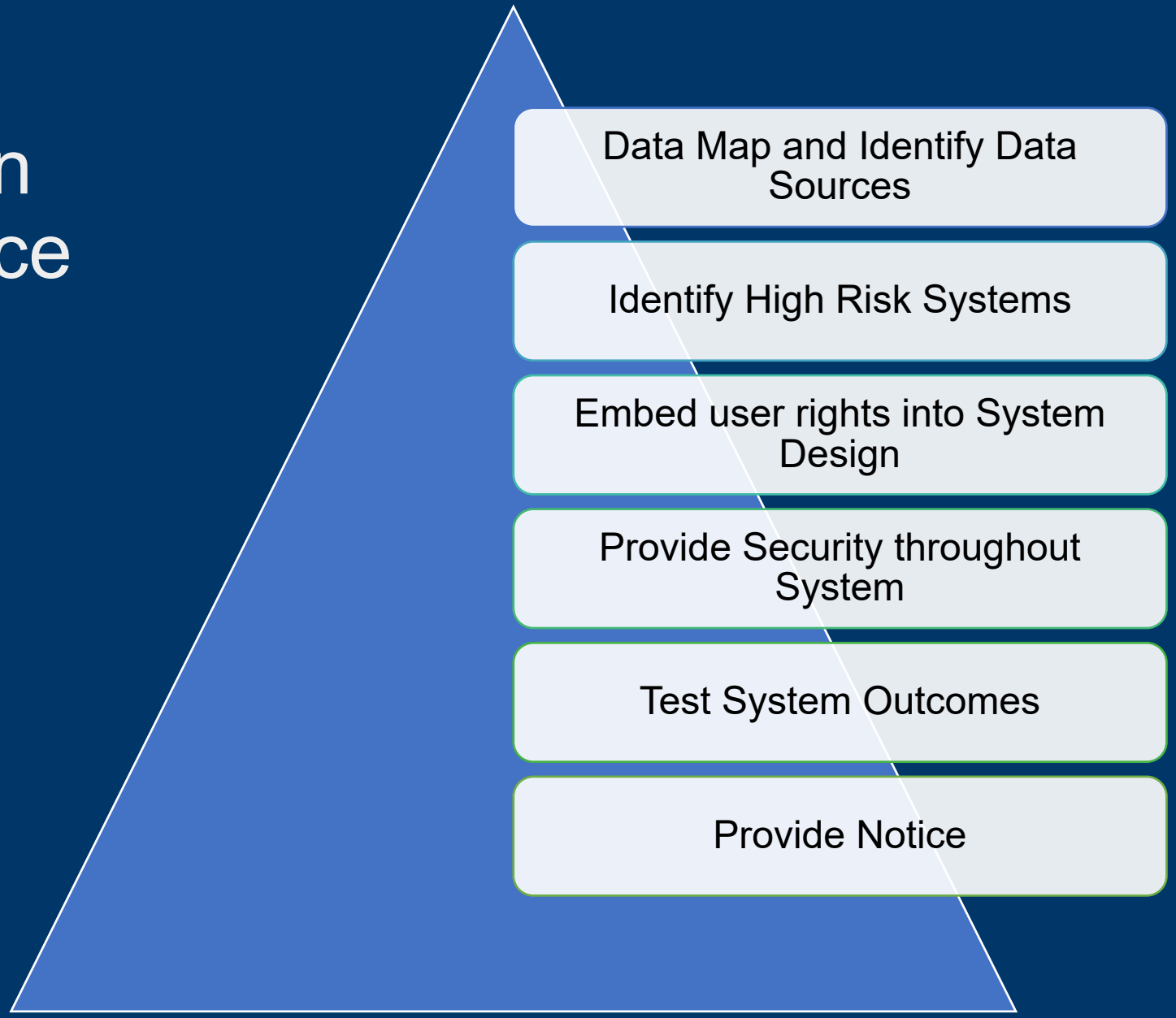
What are the unintended consequences?

Is there a risk of discrimination?

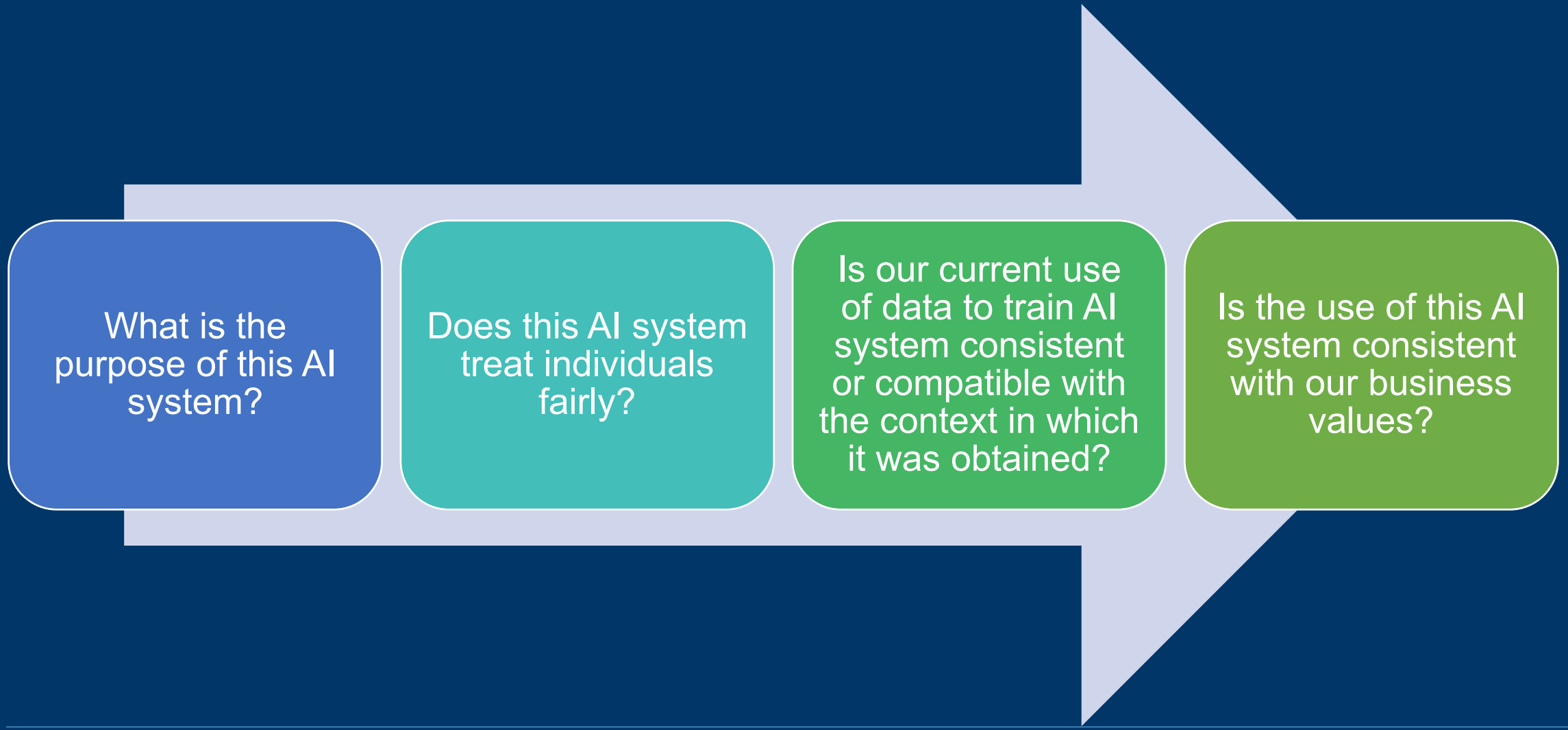
What data governance tools are available to minimize harms?

What tools do we have to audit our vendors and our outcomes?

Implementing Privacy by Design into AI Governance



Ethical Considerations



QUESTIONS?