MORRISON FOERSTER

ACC Association of Corporate Counsel SAN FRANCISCO BAY AREA

2023 Life Sciences Conference

Artificial Intelligence in Life Sciences: The Evolving Legal & Regulatory Landscape

PRESENTED BY

Brigid Bondoc
Morrison Foerster
Partner
Washington, D.C.

Wendy Chow
Morrison Foerster
Of Counsel
San Francisco

Anna Yuan
Morrison Foerster
Associate
San Francisco

Lauren Wu
Evidation Health
Head of Privacy, Sr. Dir. of Legal for Regulatory and Compliance, US Privacy Officer and Global DPO

May 11,2023

Today's Speakers

Brigid Bondoc
Morrison Foerster
Partner, Washington, D.C.
BBondoc@mofo.com

Wendy Chow
Morrison Foerster
Of Counsel, San Francisco
WChow@mofo.com

Anna Yuan
Morrison Foerster
Associate, San Francisco
AYuan@mofo.com

Lauren Wu
Evidation Health
Head of Privacy

Agenda

- Protecting AI Technology in Life Sciences
- FDA Regulatory
- Privacy and AI

Protecting AI Technology in Life Sciences

International AI Patent Filing Trend

“Patent families related to AI application fields emerged in the 1990s.”

“[D]eep learning showed an impressive average annual growth rate of **175 percent** from 2013 to 2016.”

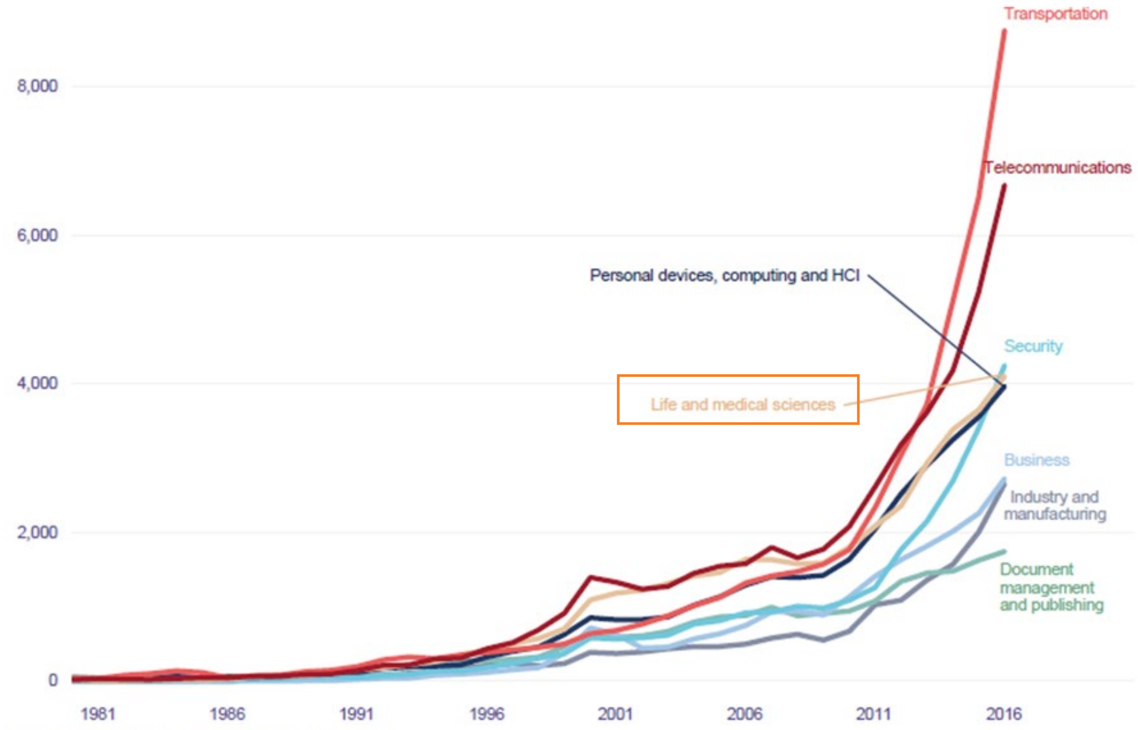


Figure 3.18. Patent families for top application field categories by earliest priority year

Patent families related to AI application fields emerged in the 1990s, with transportation and telecommunications overtaking all other fields

Note: A patent may refer to more than one category

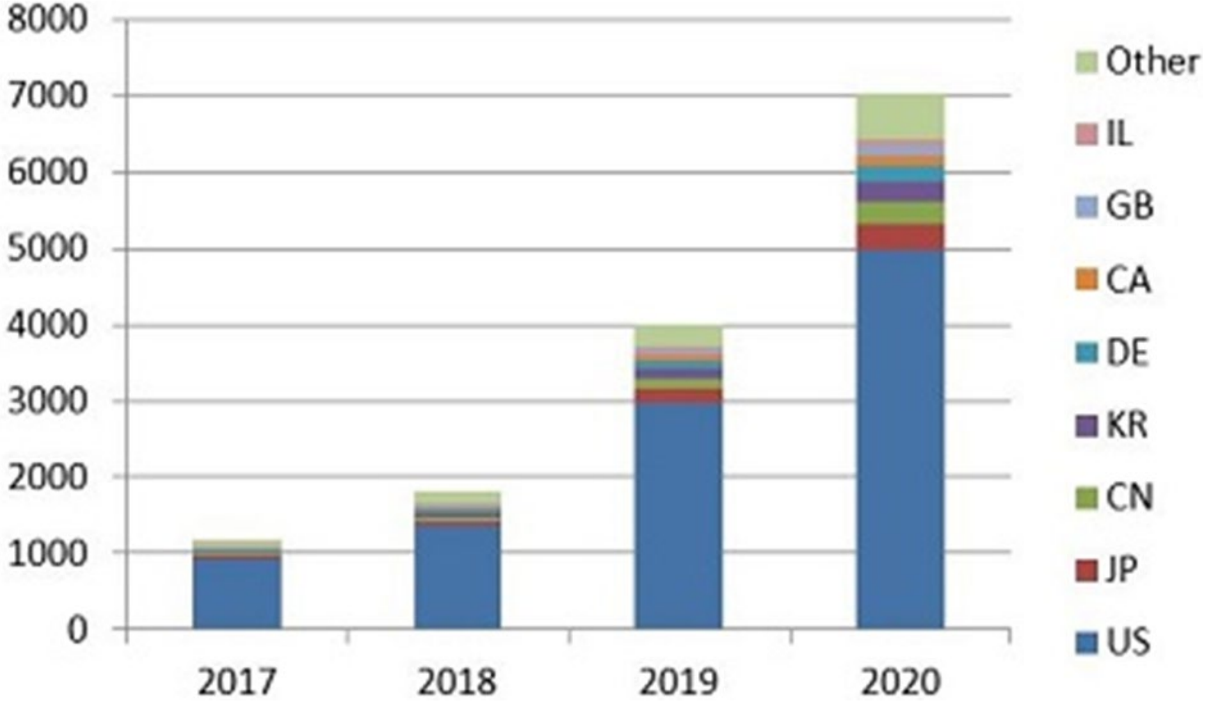
WIPO Technology Trends 2019: Artificial Intelligence, https://www.wipo.int/tech_trends/en/artificial_intelligence/

Recent AI Patent Filing Trend in the U.S.

~8x increase in AI patents from 2017 to 2020.

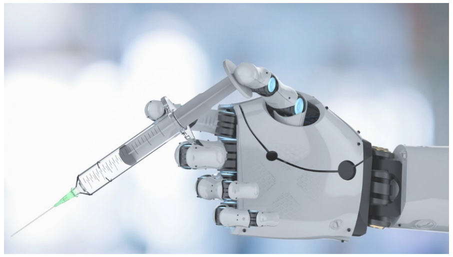
Higher percentage of **non-U.S. applicants**.

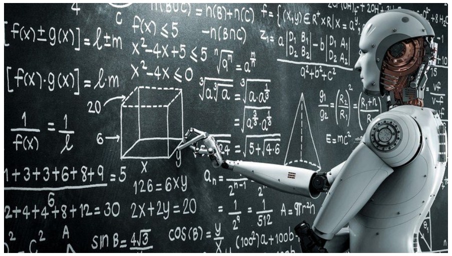
AI Patents in the U.S. by Applicant Country By Year



United States: AI Patent Trends In The U.S. Patent Office: Is The U.S. Losing Its Lead?
https://www.mondaq.com/unitedstates/patent/1041332/ai-patent-trends-in-the-us-patent-office-is-the-us-losing-its-lead

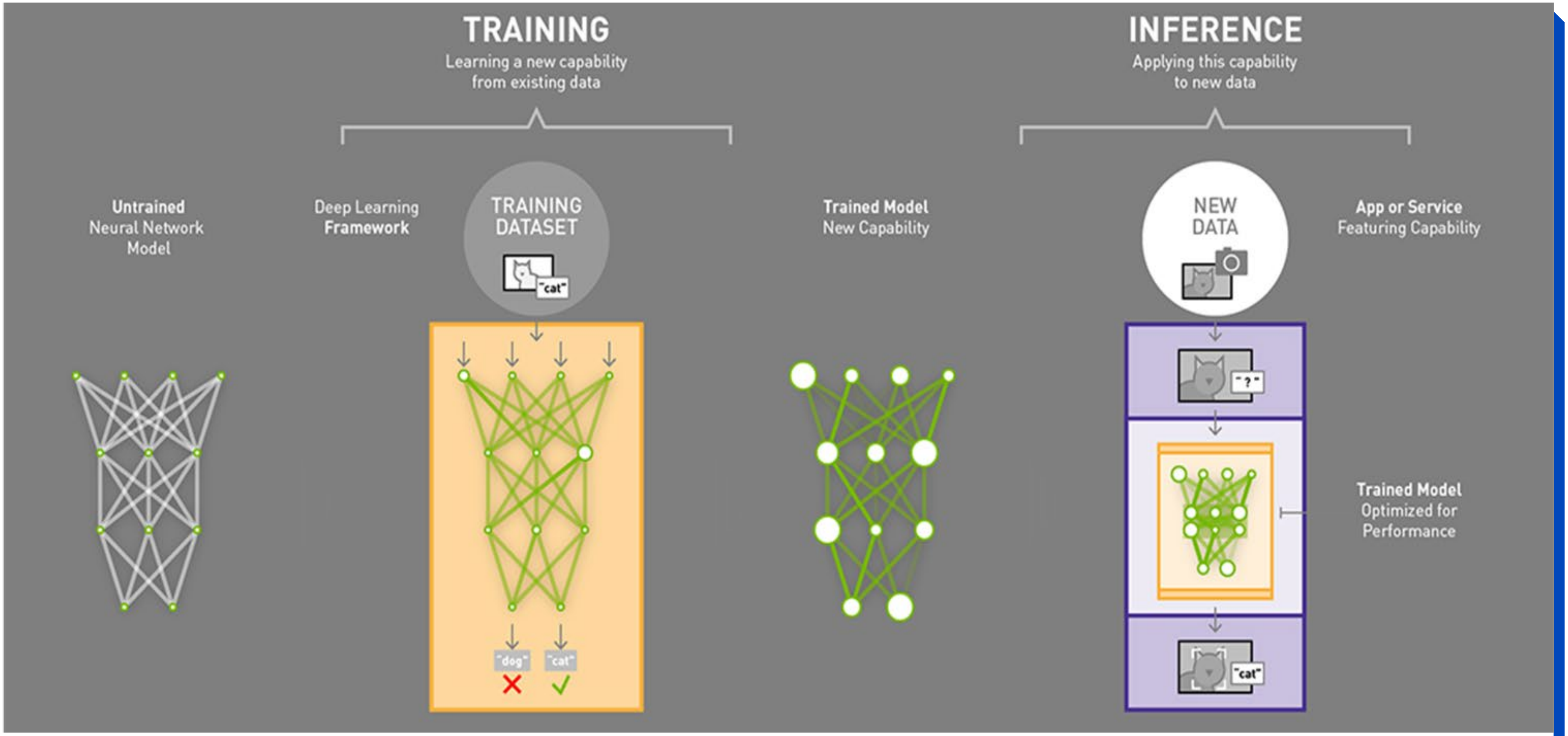
What Can Be Patented?





- **Application of known AI to specific fields and sectors**
  - E.g., achieving a new/better outcome using ML in various life sciences context (e.g., discovery of new drug, clinical trial design, medical devices, robotic surgery, medical imaging, precision medicine, healthcare and patient monitoring)
  - **Higher value** because it is likely to be detectable and can be broad
  - **This is where we pursue most of the patent applications**
- **New AI models and algorithms**
  - **Lower value** due to difficulty in detecting infringement
  - May be more difficult to patent without linking to a technical application

AI Basics and Where Innovations Can Occur


TRAINING
Learning a new capability from existing data
INFERENCE
Applying this capability to new data
Untrained Neural Network Model
Deep Learning Framework
TRAINING DATASET
"cat"
"dog"
"cat"
Trained Model New Capability
NEW DATA
App or Service Featuring Capability
"?"
Trained Model Optimized for Performance
"cat"

Choice and configuration of the model (e.g., inputs, outputs, layers)

Structure / preprocessing of training data

How the trained model is used (e.g., making a diagnosis, administering a treatment, formulating clinical trials), outputs of the model (e.g., new chemical compounds)

Patent v. Trade Secret v. Copyright

Patent

- Patents protect new, useful, and non-obvious ideas.
- **AI Examples**: an AI-based algorithm, a device executing AI techniques, a drug developed by AI, computer hardware configuration and optimization, etc.
- Need to file patent applications at various patent offices.

Trade Secret

- Trade secrets protect confidential information that provides a competitive advantage due to its secrecy.
- **AI Examples**: software code and other aspects of AI that can be kept confidential.
- Need to make a reasonable effort to maintain secrecy (e.g., by implementing trade secret policy).

Copyright

- Copyrights protect original textual works and visual or artistic expressions.
- **AI Examples**: software code, graphical user interfaces.
- Registration is optional.

Patent v. Trade Secret

- A **hybrid** approach is typically advisable:
  - Patent: practical application of AI algorithms
  - Trade secret: low-level implementation details, fine-tuning, and optimization
- Patents are especially important in competitive fields such as AI
  - **Business Goals**
    - Obtain funding and increase valuation
    - Increase brand recognition
    - Value of a monopoly on the patented technology
  - **Competitive Landscape**
    - Independent development/reverse engineering
    - Defensive filings
  - **Feasibility of Trade Secret Protection**
    - Detectability: user-facing vs. internal, secret use
    - Pitching investors
    - Selling and marketing
    - Disclosure to development partners
    - Regulatory disclosure requirements
    - Whitepapers, conference presentations, blogs
    - Employee attrition
    - Hacking and cybersecurity

FDA Regulatory

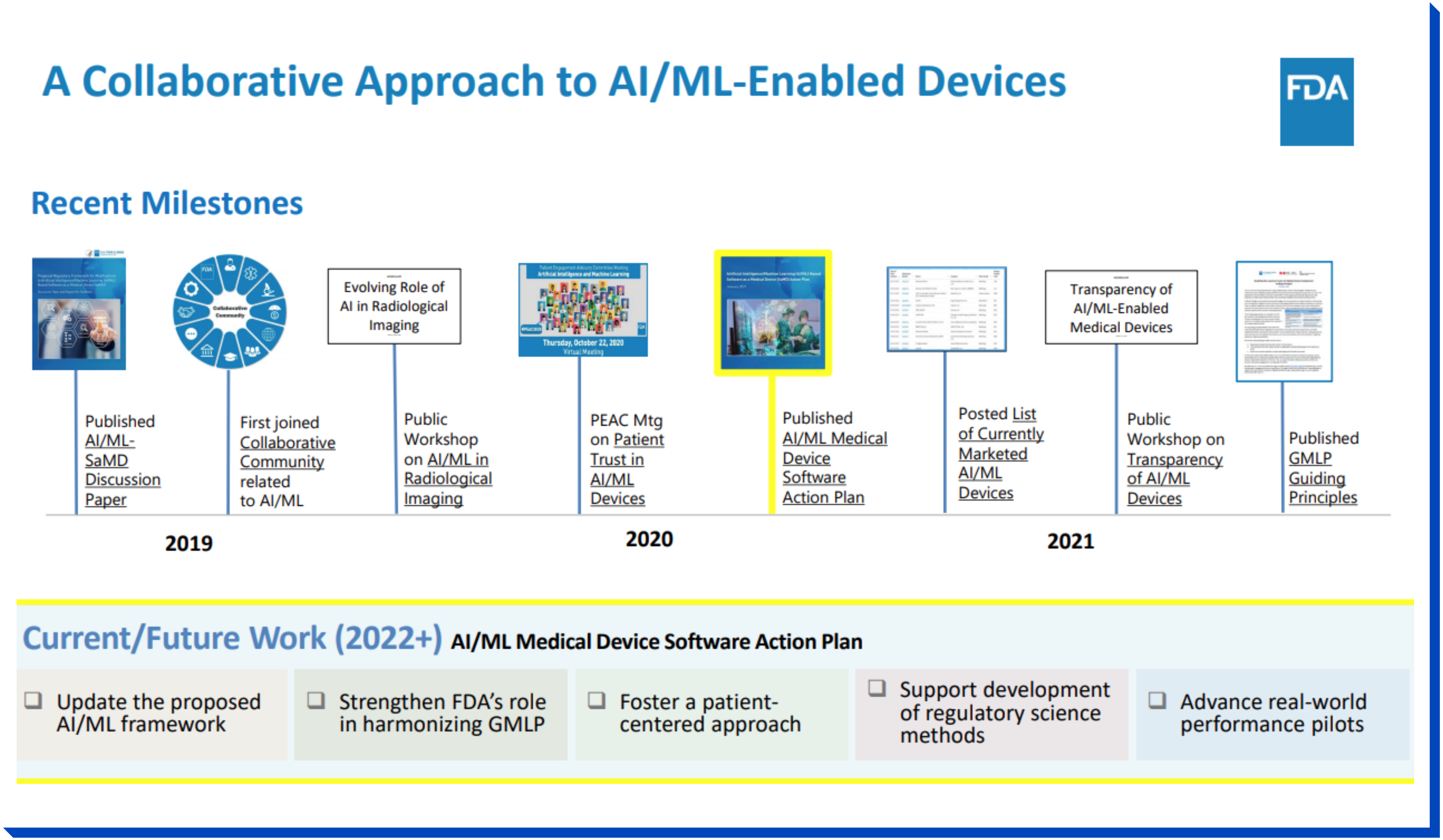
FDA Regulation of Artificial Intelligence

Current and future applications of AI may include FDA-regulated activities:

- Automation and learning of medical devices
- Efficiency of diagnostic/therapeutic development
- Regulatory assessment
- Post-market surveillance

FDA is actively monitoring the use of AI and ML software in medical devices and clinical developments and has taken some first steps in building its regulatory framework.

AI/ML – FDA Milestones



A Collaborative Approach to AI/ML-Enabled Devices

FDA

Recent Milestones

Evolving Role of AI in Radiological Imaging

Transparency of AI/ML-Enabled Medical Devices

2019

- Published AI/ML-SaMD Discussion Paper
- First joined Collaborative Community related to AI/ML
- Public Workshop on AI/ML in Radiological Imaging

2020

- PEAC Mtg on Patient Trust in AI/ML Devices
- Published AI/ML Medical Device Software Action Plan

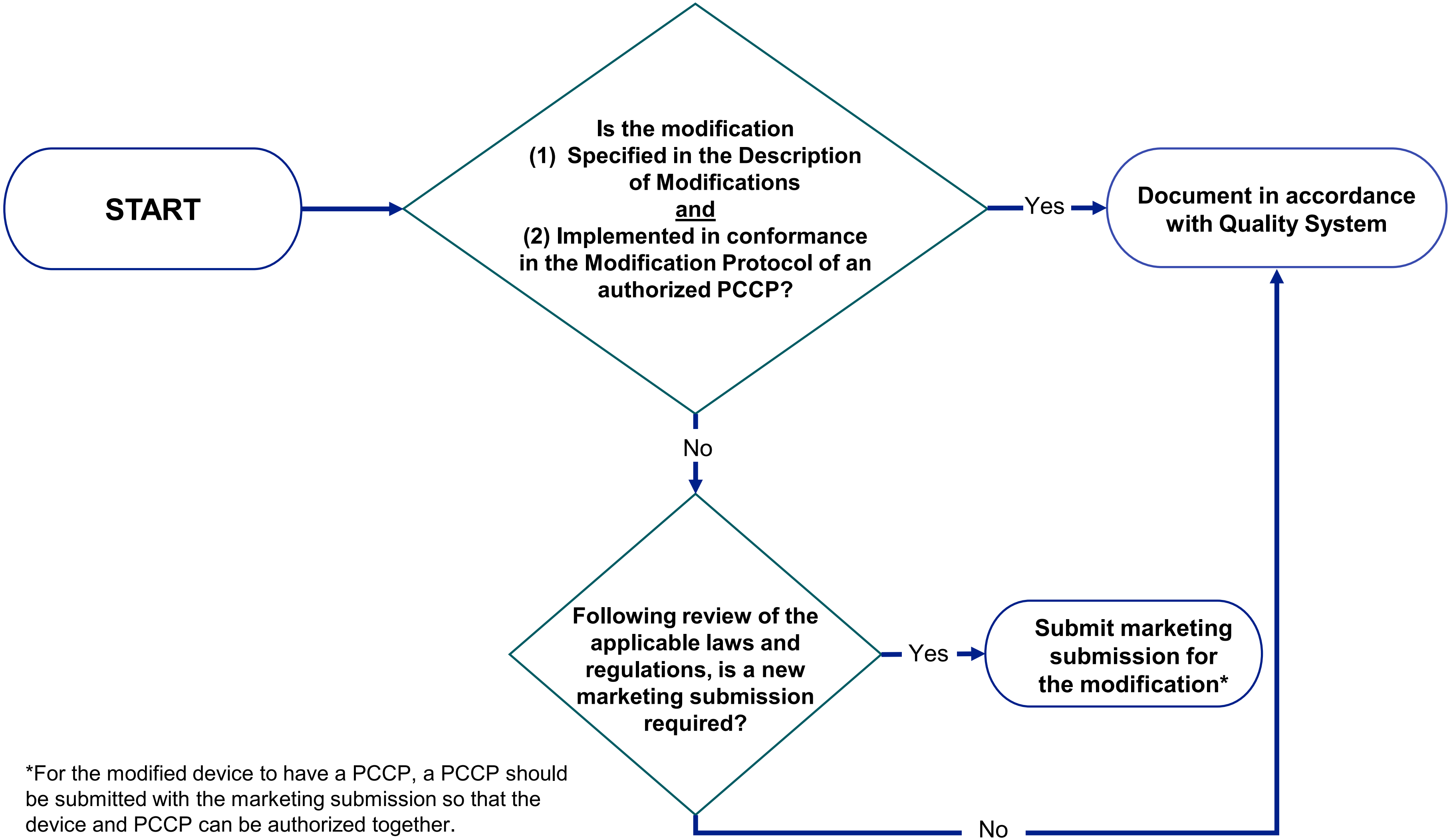
2021

- Posted List of Currently Marketed AI/ML Devices
- Public Workshop on Transparency of AI/ML Devices
- Published GMLP Guiding Principles

Current/Future Work (2022+) **AI/ML Medical Device Software Action Plan**

- ❑ Update the proposed AI/ML framework
- ❑ Strengthen FDA's role in harmonizing GMLP
- ❑ Foster a patient-centered approach
- ❑ Support development of regulatory science methods
- ❑ Advance real-world performance pilots

Draft Guidance - Predetermined Change Control Plan for AI/ML-Enabled Device Software Functions


START
Is the modification
(1) Specified in the Description of Modifications
and
(2) Implemented in conformance in the Modification Protocol of an authorized PCCP?
Yes
Document in accordance with Quality System
No
Following review of the applicable laws and regulations, is a new marketing submission required?
Yes
Submit marketing submission for the modification*
No

*For the modified device to have a PCCP, a PCCP should be submitted with the marketing submission so that the device and PCCP can be authorized together.

MORRISON FOERSTER

Bias and Transparency in AI/ML-Enabled Medical Devices

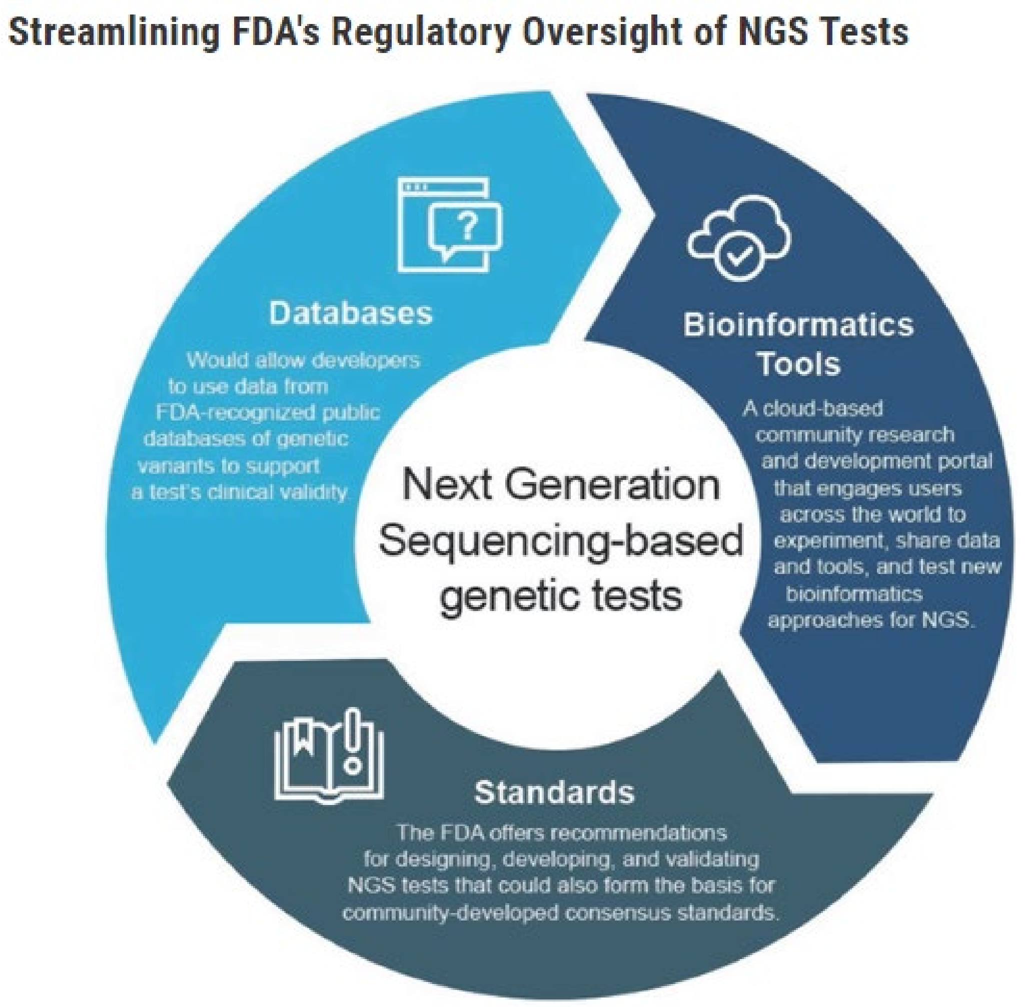
FDA has been focused on addressing bias in AI/ML-enabled medical devices and the role of transparency in enhancing safety and effective use of this new technology.

FDA held a virtual public workshop on transparency in October 2021 to discuss bias and transparency in AI/ML-enabled devices

- Bias and systemic discrimination are persistent issues in the AI/ML space. FDA has expressed ongoing commitment to ensure data used to train AI/ML models are diverse and accurately reflective of the patient population.
- FDA and industry stakeholders emphasized the need for transparency and effective communication in AI/ML-enabled medical device labeling

FDA has not addressed potential bias and transparency issues related to AI/ML-enabled drug development.

Pharmacogenetics and Next Generation Sequencing



Streamlining FDA's Regulatory Oversight of NGS Tests

Next Generation Sequencing-based genetic tests

Databases

Would allow developers to use data from FDA-recognized public databases of genetic variants to support a test's clinical validity

Bioinformatics Tools

A cloud-based community research and development portal that engages users across the world to experiment, share data and tools, and test new bioinformatics approaches for NGS.

Standards

The FDA offers recommendations for designing, developing, and validating NGS tests that could also form the basis for community-developed consensus standards.

5 Software Types Not Medical Device

5 Types of Software excluded from “device” definition:

- Administrative support of health care facility, including lab workflow, appointment schedulers
- Maintain or encourage a healthy lifestyle, unrelated to diagnosis, cure, mitigation, prevention, or treatment of disease or condition
- Electronic patient records for transfer, store, convert formats, or display patient information (do not “interpret or analyze”) and created, stored, transferred, reviewed by professional or staff
- Transfer, store, convert formats, or display lab test or device data (MDDS)
- Clinical decision support software (discussed on next slide)

Mobile Medical Apps

Mobile apps that transform a mobile platform into a regulated medical device:

- These mobile apps use a mobile platform’s built-in features such as light, vibrations, camera, or other similar sources to perform medical device functions.
- Example: wearable tremor transducers that use a sensor attached to mobile platform to measure the degree of tremor caused by certain diseases

Software functions that are used in active patient monitoring to analyze patient-specific medical device data:

- Example: perinatal monitoring systems

Software functions that connect to an existing device type for purposes of controlling its operation, function, or energy source:

- Example: software used to calibrate hearing aids and assess frequency/sound emanating from hearing aid

TREMOR SNAPS
Analyze your tremors with detailed reports.
ANALYZE ACTIVITY
Compare how your tremors react during different activity
SHARE & COMPETE
Share your tremors & motivate yourself with challenges

Medical Device Data Systems

Medical Device Data Systems (MDDS) are hardware or software products intended to transfer, store, convert formats and display medical device data.

Non-device MDDS: Software functions that are *solely intended* to transfer, store, convert formats, and display medical device data or medical imaging data, are not devices and are not subject to FDA regulatory requirements applicable to devices.

- Non-device MDDS does NOT:
  - modify the data or display of the data
  - control the functions or parameters of other medical devices
- Example: store patient blood pressure readings for review at later time, convert digital data from pulse oximeter into printable format

Device MDDS: Hardware functions that are *solely intended* to transfer, store, convert formats, and display medical device data or results.

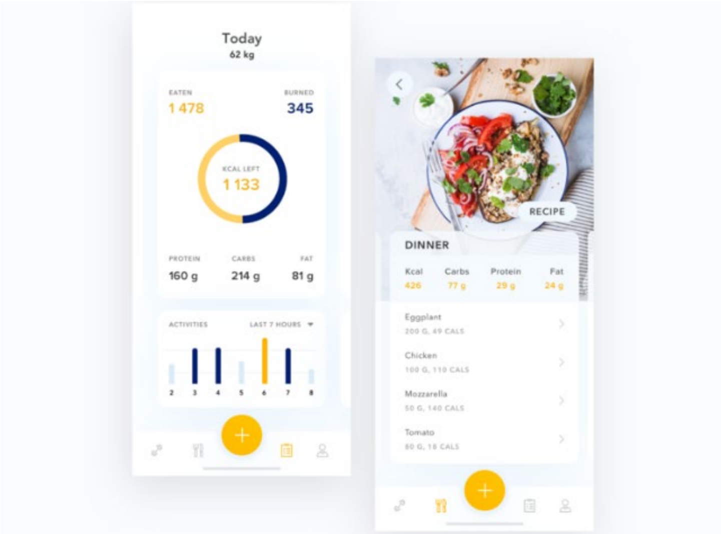
General Wellness Guidance

General Wellness Device:

Intended use is related to generally maintaining or encouraging a general state of health or a healthy activity (unrelated to any disease or condition).

Intended use that relates the role of healthy lifestyle with helping to reduce the risk or impact of certain chronic diseases or conditions.

- Only where it is well understood that healthy lifestyle has an impact on health outcomes for the disease/condition.
- Two different categories.



Today
62 kg

EATEN 1 478
BURNED 345
KCAL LEFT 1 133

PROTEIN 160 g
CARBS 214 g
FAT 81 g

DINNER			
Kcal	Carbs	Protein	Fat
426	77 g	29 g	24 g

Eggplant
200 G, 49 CALS

Chicken
100 G, 110 CALS

Mozzarella
50 G, 140 CALS

Tomato
80 G, 18 CALS

Clinical Decision Support (Exclusions)

A software function will be considered non-device CDS if it:

1. NOT intended to acquire, process, or analyze medical image or signal.
2. Intended for purpose of displaying, analyzing, or printing patient-specific medical information.
3. Intended for the purpose of supporting or providing recommendations to an HCP on prevention, diagnosis, or treatment.
4. Intended to enable HCP to independently review basis for recommendations so HCP does not rely primarily on the CDS recommendations in clinical diagnosis or treatment decisions.

All of the four criteria must be met in order for a CDS to be non-device.

Clinical Decision Support (Exclusions)

Examples of Non-Device CDS:

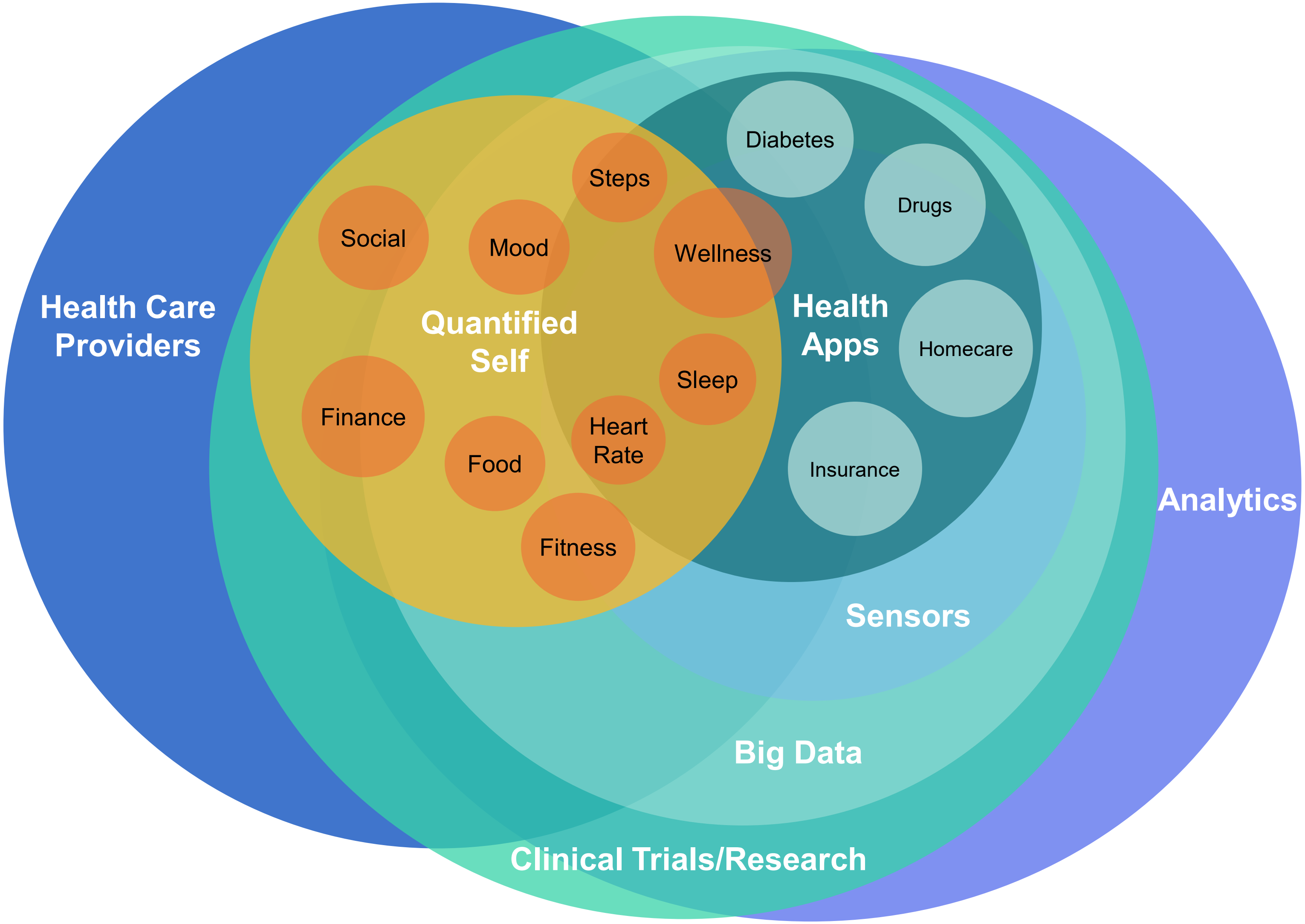
- Software function that provides an alert to notify an HCP of redundant test orders and advise discontinuation of the order
- Software function that uses medical information from the patient's medical records to provide an HCP with recommended assessments prior to discharge, such as a pain assessment
- Software function that analyzes the type of arthritis diagnosis in patient's medical record and identifies prioritized treatment options available for the condition

Examples of Device CDS

- Software function that uses patient images (e.g., MRI) to create an individual treatment plan for review by HCP
- Software function that identifies patients with possible diagnosis of opioid addiction based on analysis of patient medical information

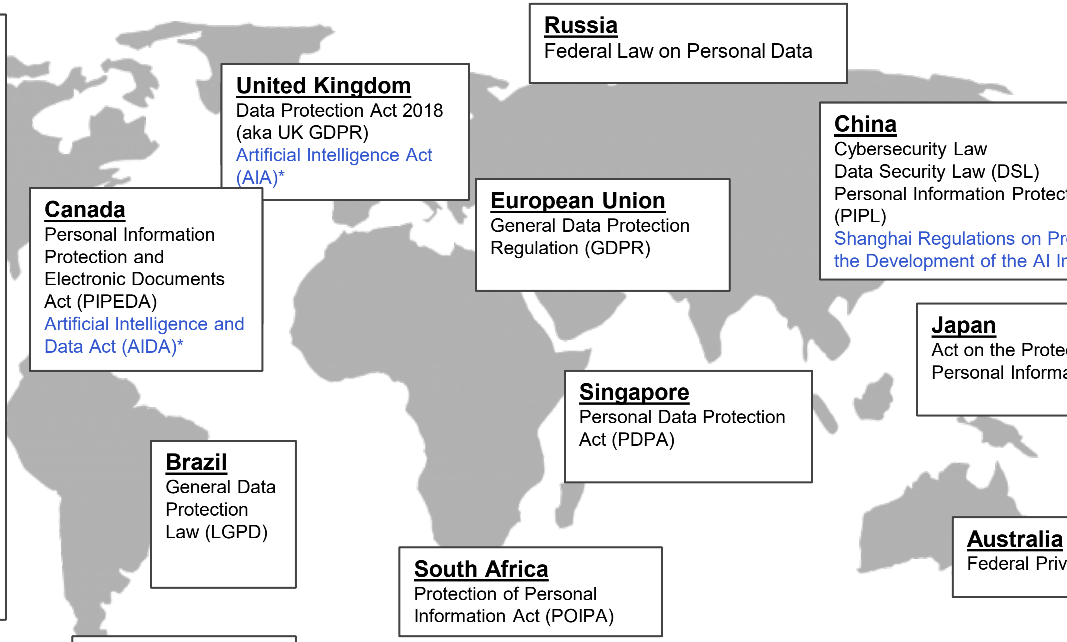
Privacy and AI

Health Data Ecosystem



Privacy & Data Protection are Global Concepts

Comprehensive privacy laws are trending in the U.S. Complimenting this paradigm shift is a focus on laws regulating AI or use of AI and inclusion of reference to Automated Decision-Making in these general privacy laws.



United States
California Consumer Privacy Act (CCPA)
Health Insurance Portability and Accountability Act (HIPAA)
Health Information Technology for Economic and Clinical Health (HITECH) Act
Children’s Online Privacy Protection Act (COPPA)
Foreign Contribution Regulation Act (FCRA)
Gramm-Leach-Bliley Act (GLB)
Telephone Consumer Protection Act (TCPA)
The Controlling Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
Genetic Information Non-Discrimination Act (GINA)
California Privacy Rights Act of 2020 (CPRA)
Virginia’s Consumer Data Protection Act (V-CDPA)
Colorado Privacy Act (CPA)
NYC AI Bias Law

***Coming Soon* in the United States**
Utah Consumer Privacy Act (U-CPA)
Connecticut Personal Data Privacy and Online Monitoring Act (CPDPA)
Washington My Health My Data Act (MYMDA)
Tennessee Information Privacy Act (TIPA)
Indiana Consumer Data Protection Act (I-CDPA)
Iowa Privacy Act (IPA)
Montana Consumer Data Privacy Act (M-CDPA)

United Kingdom
Data Protection Act 2018 (aka UK GDPR)
Artificial Intelligence Act (AIA)*

Canada
Personal Information Protection and Electronic Documents Act (PIPEDA)
Artificial Intelligence and Data Act (AIDA)*

Brazil
General Data Protection Law (LGPD)

Argentina
Personal Data Protection Law (PDPL)

Russia
Federal Law on Personal Data

European Union
General Data Protection Regulation (GDPR)

South Africa
Protection of Personal Information Act (POIPA)

Singapore
Personal Data Protection Act (PDPA)

China
Cybersecurity Law
Data Security Law (DSL)
Personal Information Protection Law (PIPL)
Shanghai Regulations on Promoting the Development of the AI Industry

Japan
Act on the Protection of Personal Information (APPI)

Australia
Federal Privacy Act 1988

The addition of restrictions on use of automated decision-making is generally to ensure transparency and awareness, fairness, and avoiding bias / discrimination, especially when the outcome of the decision could impact an individual’s rights.

Key Privacy Laws Regulating AI: U.S.

Patchwork of federal privacy laws based on AI methods and uses:

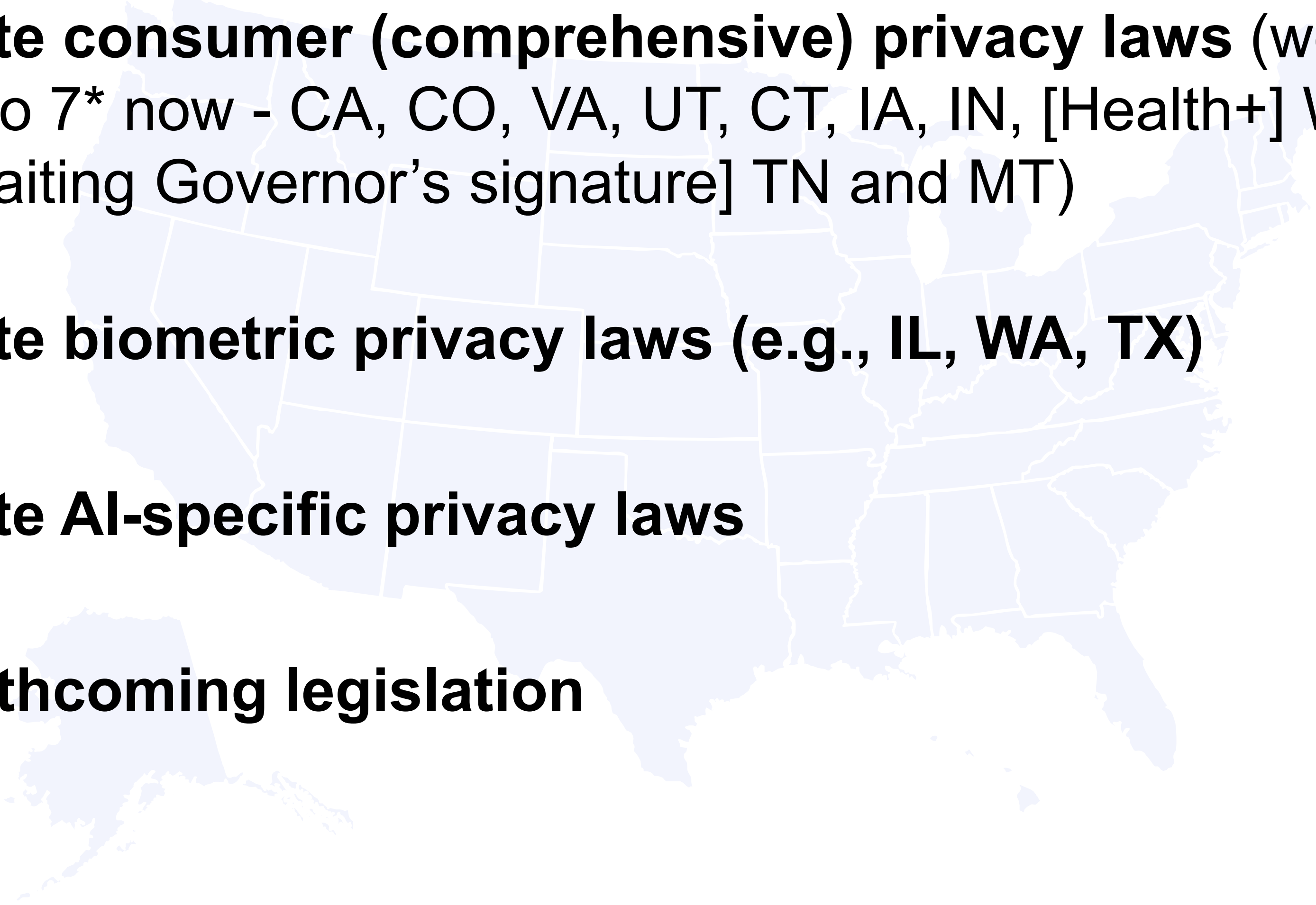
- **Health information laws**
  - Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA)
  - State health information laws similar to HIPAA (e.g. CA, TX)
- **Federal consumer protection laws, depending on use of AI**
  - Section 5 of Federal Trade Commission Act
  - *See* FTC guidance, “Aiming for truth, fairness, and equity in your company’s use of AI” (2021)
  - FTC 2022 Settlement with "Weight Watchers" (Kurbo, Inc, / W.W. International) and “algorithmic disgorgement”
- **Federal guidance and more**
  - NIST AI guidance
  - AI Bill of Rights

AI and HIPAA

HIPAA

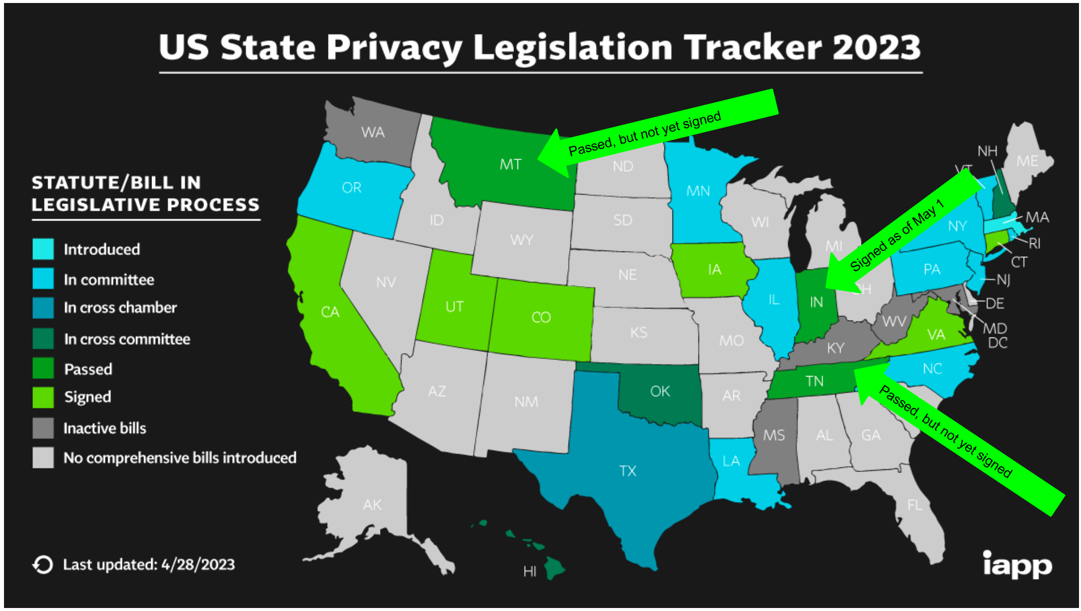
- **Applies to covered entities and business associates**
  - In the space of digital health and many medical devices, more likely these will be “HIPAA adjacent”
  - For AI developers, however, working in the traditional health care space seems inevitable
  - Certain state health information laws also are broadening their reach
- **HIPAA covered entities may use and disclose PHI for “treatment,” “payment,” “health care operations”**
  - AI can fall within and be beneficial in all of these activities
- **HIPAA business associates have access to PHI when acting on behalf of their covered entity customers**
  - Business associates may provide AI-related services
  - BAA limitations and interpretation of “proper management and administration”

State Patchwork of Privacy Laws



- **State consumer (comprehensive) privacy laws** (we’re up to 7* now - CA, CO, VA, UT, CT, IA, IN, [Health+] WA, [awaiting Governor’s signature] TN and MT)
- **State biometric privacy laws (e.g., IL, WA, TX)**
- **State AI-specific privacy laws**
- **Forthcoming legislation**

New U.S. State Privacy Law Compliance



Passed, but not yet signed

Signed as of May 1

Passed, but not yet signed

5 *new* comprehensive state privacy laws are already in effect or coming into effect in 2023…More are already on the horizon.

Plus a new “health data” law in WA

Privacy Issues to Consider When Using AI in Health Care and Life Science

- AI algorithms involve:
  - Collection and use of data, including personal information (PI), for initial training of algorithms and updating algorithms – *Is the use permissible under applicable law?*
  - Potential secondary uses of data for purposes beyond the initial purpose of collecting data, including new and novel purposes – *Are secondary uses contemplated and permissible?*
  - AI models are can provide “black box” decision making - *How does the “black box” AI model inform use and processing of personal information?*
- Developers of AI have responsibility to create AI algorithms that adhere to legal and regulatory requirements
- Corporate users of AI technologies also have responsibility to deploy AI technologies in accordance with legal and regulatory requirements

What Issues Are AI Developers and AI Customers Negotiating in Their Contracts?

- Use of de-identified data: shifting the risk for potential re-identification
- Identifying high-risk use of models in health care: clinical trials, coding and billing, clinical decision support, software as a medical device
- Who is responsible for “controls” for upstream customers and users
- Indemnities are key

Common Privacy Principles for AI

1 Accountability

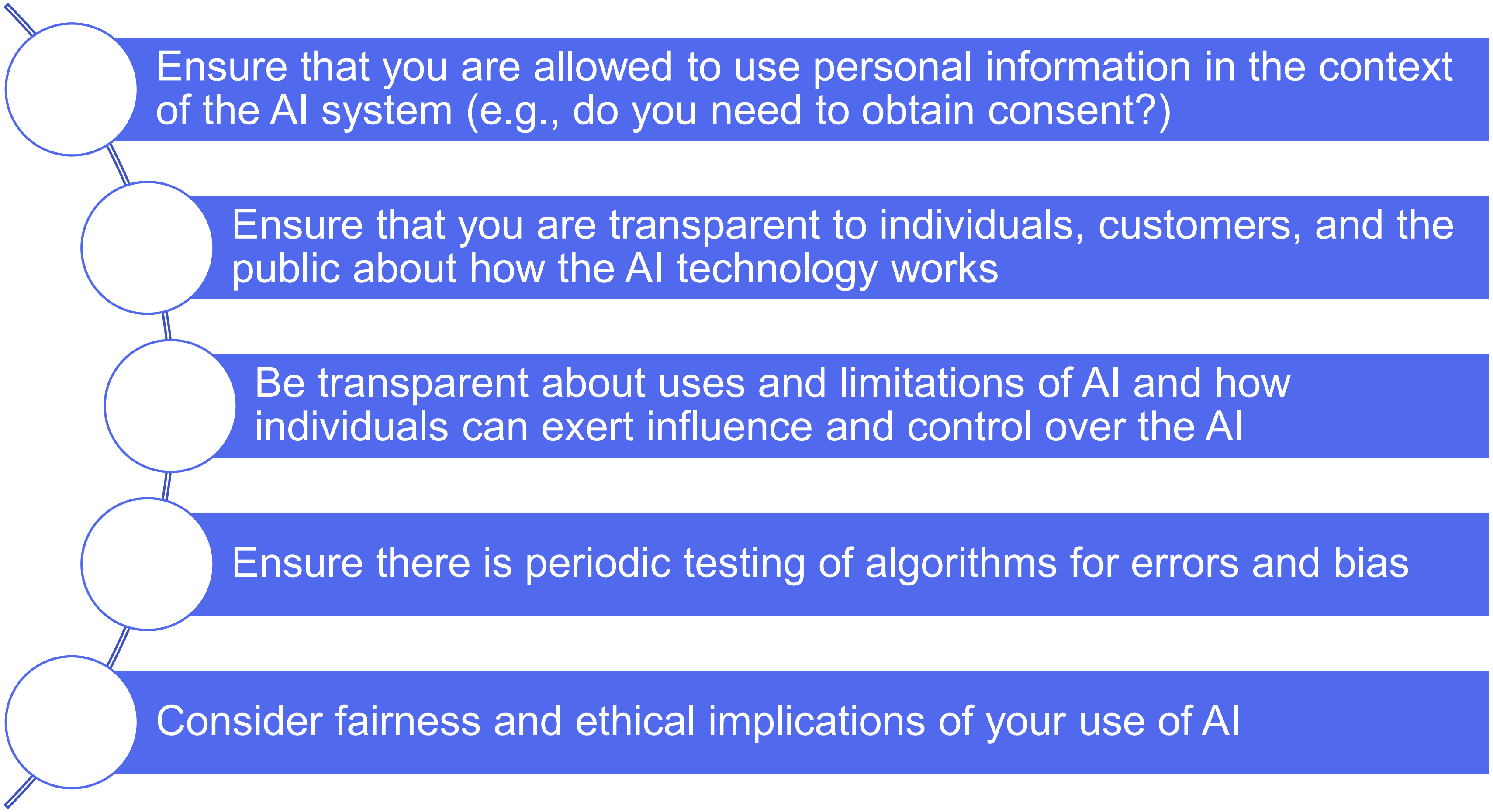
2 Explainability

3 Transparency

4 Preventing bias

5 Fairness

AI Privacy Best Practices



Ensure that you are allowed to use personal information in the context of the AI system (e.g., do you need to obtain consent?)

Ensure that you are transparent to individuals, customers, and the public about how the AI technology works

Be transparent about uses and limitations of AI and how individuals can exert influence and control over the AI

Ensure there is periodic testing of algorithms for errors and bias

Consider fairness and ethical implications of your use of AI

MORRISON FOERSTER

Thank you

Subscribe to the MoFo Life Sciences Blog for timely legal and business insights and in-depth analyses on trends and the complex technologies at the heart of the global life sciences industry.

lifesciences.mofo.com

Appendix

Contractual Considerations in AI Deals

IP Ownership and Protection

- While each AI discipline is different in its specific implementation, a number of themes are common to many modern AI Systems that given rise to particular IP questions:
  - By replicating aspects of human cognition, AI systems have the potential to engage in acts of content creation – *can an AI system be an author of a work?*
  - Many AI systems, in particular those using machine learning techniques, undergo a training process in which they develop their own decision-making capabilities / algorithms and rules by practicing decision making and using feedback to improve future decisions – *if the algorithms change over time, is the original author the owner of the developed algorithms?*
  - Training AI systems often requires large volumes of training data to ensure the system develops its decision-making algorithms based on the data that reflects the full range of scenarios it may encounter in operation – *if a third party owns the data, who is the output of the system owned by?*
  - AI systems are often used to sift through large volumes of input data to detect statistical features or patterns – *is the author the person who designed the AI system? The author/source of the input data? Neither?*

Liability Concerns

Shift in Liability Concerns

From a contractual perspective, new issues to consider with respect to AI/machine learning technology

- Current contracting models generally account for failures based on human error
  - SLAs focus on standardizing level and quality of service personnel
  - Data protection and security provisions often backed by audit and inspection rights, focusing on oversight and monitoring of human error
  - Liability exclusions address human-based errors, including gross negligence and willful misconduct
- AI/machine learning services have different failure concerns
  - General risk associated with use of framework in its development stage
  - Greater risk of large-scale “catastrophic” failures, as errors may accumulate rapidly and be caught less frequently
  - Lack of oversight into internal processes of framework and how it functions with newly input data
  - Less control of data ingested into framework, including risk of pollution with “bad” training data

Liability Concerns: Contractual Allocation

Questions to Consider From a Contractual Perspective

- Who is liable for the acts of the AI framework (e.g., the core algorithm owner, the data provider, the user)?
- On what basis will liability need to be decided (e.g., vicarious liability, strict liability)?
- What types of failure modes must the service provider protect against?

Suggested Contractual Protections for Service Provider

- Broad liability disclaimers that account for:
  - errors and inaccuracies resulting from use of the core algorithm,
  - loss or corruption of service recipient’s data through use of algorithm,
  - service recipient’s reliance and actions based on output of algorithm.
- Strict capping of liability and disclaiming of indirect and consequential damages
- No obligations to indemnify service recipients for any harm incurred through use of algorithm
- Limitations on service recipient’s remedies (e.g., limited to service provider’s making commercially reasonable efforts to correct errors)

Common Elements of Commercial Terms and Data Ownership

Terms tend to be provider-favorable

- Unilateral right for provider to terminate services
- Broad disclaimers for provider's liability
- Broad one-way indemnity obligations
- Capping of provider's liability
- Strict usage requirements on the customer
- Provider's right to modify or cancel the services at any time
- Broad disclaimers for results of machine-learning systems
- Broad rights for provider to use input data to improve the services
- Limitations on customer's rights to use output data

Data ownership is defined by the extent to which it reflects the customer's original input data

- Output data from which input data cannot be identified, commonly owned by provider
- Broad rights for provider to exploit data
- Customer takes full responsibility for input data