Potential Data Privacy and AI Risks in the Product Life Cycle of a Medical Device

Bernadette M. Broccolo
Partner
McDermott Will & Emery LLP
312.984.6911
bbroccolo@mwe.com

Presentation Focus

- Data Compliance and Liability Risks and Challenges
  - Data Integrity
  - Privacy and Security Risk Challenges
- Special Patient-Safety Related Compliance and Liability Risk Challenges
  - FDA Medical Device Regulation Compliance
  - Malpractice Liability
  - Product Liability
  - Consumer Transparency / Fraud and Deception

Understanding AI Technology

"[E]ven though we make these networks, we are no closer to understanding them than we are a human brain"

Davide Castelvecchi, *Can We Open the Black Box of AI?*, NATURE (Oct. 5, 2016) (quoting an AI Researcher)

"Machine-learning algorithms may be black boxes, even to their creators and users"

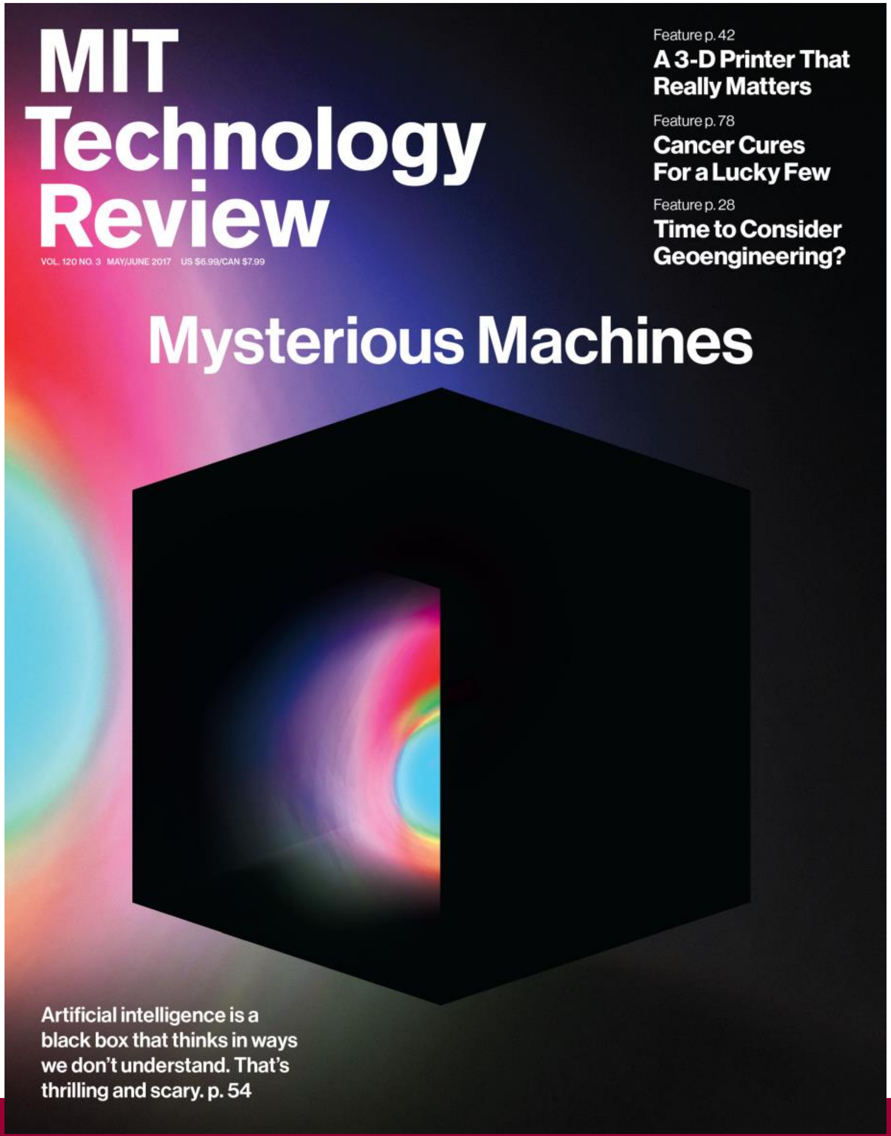
Yavar Bathaee, "The Artificial Intelligence Black Box And The Failure Of Intent And Causation," *Harvard Journal of Law and Technology* (Spring 2018)

. . . AND THEN THE OTHER VIEW . . .

". . . beyond the promise lies the truth: What people term as AI is 'basically really simple algorithms running on Big Data sets, and the most powerful ones actually … just do pattern recognition . . .' "

- *Mark Jamison, Global Head of Innovation at Visa*

"Artificial Intelligence is a 'black box' that thinks in ways we don't understand. That's thrilling and scary."



Feature p. 42

A 3-D Printer That Really Matters

Feature p. 78

Cancer Cures For a Lucky Few

Feature p. 28

Time to Consider Geoengineering?

MIT Technology Review

VOL. 120 NO. 3 MAY/JUNE 2017 US $6.99/CAN $7.99

Mysterious Machines

Artificial intelligence is a black box that thinks in ways we don't understand. That's thrilling and scary. p. 54

*The "**Black Box**" concept refers to **Software that does not explain how the input data are analyzed in order to come to a recommendation** because either:*

- *It is **too complex** to be understood by humans*

- OR -

- *The owner protects that information as a **proprietary trade secret**.*

Compliance and Liability Risks Planning Considerations

- Managing compliance and liability risks is more challenging in the realm of healthcare AI than other forms of digital health.
  - AI technology and solutions are more varied, which creates a wider range of facts and circumstances to address through compliance measures.
  - Many of the applicable laws and regulations pre-date the development of Artificial Intelligence – they were written without the “black box” dimension of AI in mind.
  - Adaptation of the Law to this brave new world of healthcare technology lags behind the pace of AI innovation.

Compliance and Liability Risks Planning Considerations

- These risks are relevant to Medical Device companies because they either:
  - Arise from laws and regulations directly applicable to Medical Device Companies, or
  - They arise indirectly through Medical Device Companies' contractual relationships with other companies (e.g., hospitals, physicians) to which the laws and regulations directly apply.

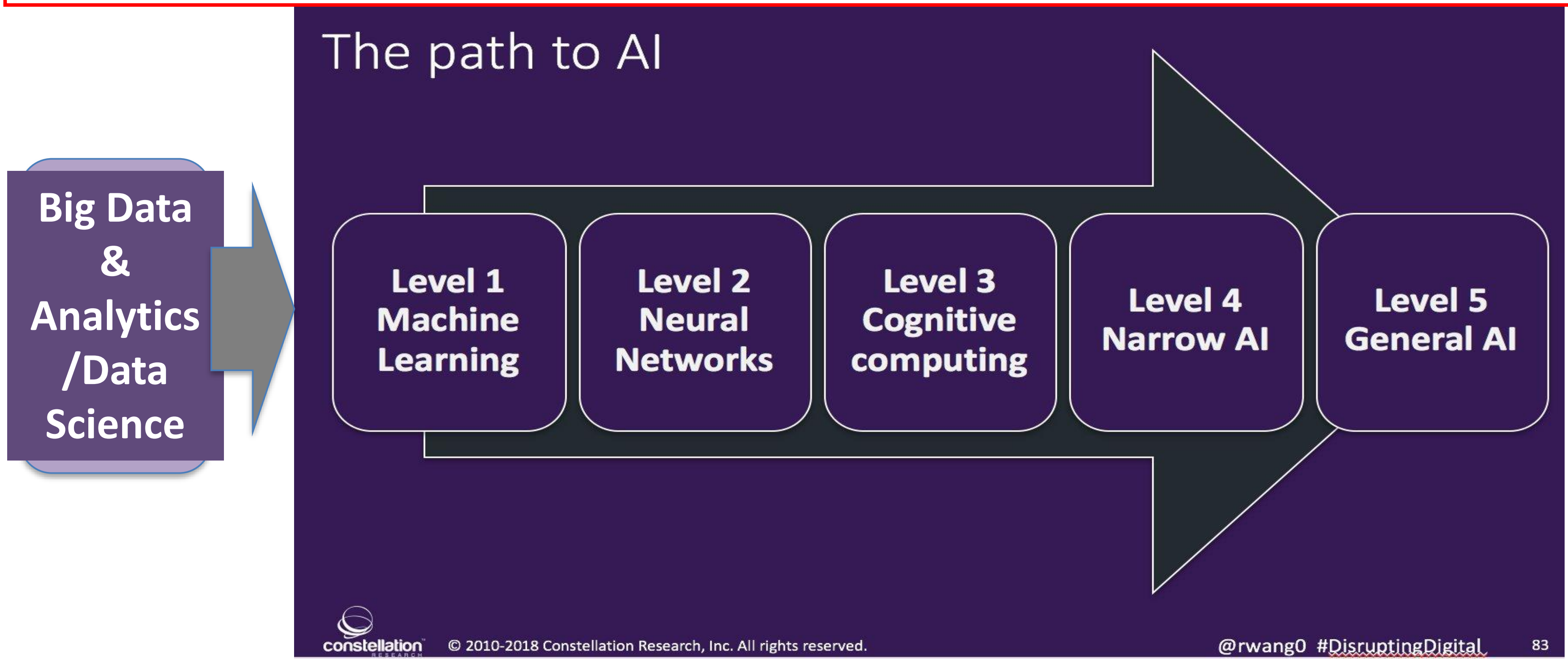
Compliance and Liability Risks Planning Considerations

- ***[T]he law is presently at an inflection point, as never before has the law encountered thinking machines.”***
- *“. . . the law is built on legal doctrines that are focused on human conduct, which when applied to AI, may not function . . .*
- *[T]he doctrines that pose the greatest risk of failing are two of the most ubiquitous in American law —* ***intent and causation*** *. . .*

Yavar Bathaee, “The Artificial Intelligence Black Box And The Failure Of Intent And Causation,” *Harvard Journal of Law and Technology* (Spring 2018)

AI Technology Sophistication v. Degree of Legal Risk

The degree compliance regulation and liability risk increases as (a) AI technology come closer to highly sophisticated "black box" technology that does not enable independent clinician review of the basis for the recommendation or solution, and (b) the AI-generated recommendations come closer to being the primary or sole basis for a diagnosis or treatment.



© 2010-2018 Constellation Research, Inc. All rights reserved.

Data Quality, Reliability and Analyzability Challenges

The integrity and reliability of an AI algorithm's results and recommendations, and of the corresponding medical decisions made using such AI input, depend largely on the quality, reliability and analyzability of the massive data required to train AI algorithms.

> *". . . for all their enormous potential, A.I.-powered systems have a dark side. Their decisions are only as good as the data that humans feed them . . . ."*
>
> Vanian, J., "Unmasking A.I.'s Bias Problem," FORTUNE (June 25, 2018), *available at* http://fortune.com/longform/ai-bias-problem/

Data Quality, Reliability and Analyzability Challenges

- **Data used by many AI algorithms typically is Robust and Multi-Dimensional**:
  - Consists of various **categories/types** of data,
  - Is stored/organized in various **forms** (both structured and unstructured),
  - Comes from **multiple sources**, some regulated, some not, such as:
    - Other providers,
    - Patients/Consumers (through the internet and using personal wearables and mobile devices),
    - Other large repositories,
    - Literature, and
    - Other Publicly Available Sources.
- This in turn creates **variations quality and reliability**.

Data Quality, Reliability and Analyzability Challenges

- **Standards are lacking** as to consistency, accuracy and interoperability across Big Data sources and settings.
  - Lack of interoperability between and among information systems.
  - Ongoing standards development is required to link patient data
- **Integrating, comparing and analyzing** robust and highly varied data is challenging.
- **De-identifying Data** may diminish the value of the data because de-identification can neutralize important information

  (e.g., geographic, economic and social determinants of health) and introduce biases.
- **Synthetic Data** may help de-identification but has analytical limitations.
  - No consensus on how to create synthetic data.
  - Replication of general trends in underlying data may diminish the ability to predict specific trends within a data set.
- **Validating** data integrity may become increasingly difficult over the full life cycle of **continuous learning AI**

Data Quality, Reliability and Analyzability Challenges

Potential for Introduction of Bias

- Data reflecting natural conscious or unconscious human biases of the providers who created the data (sexism, racism)
- Data that fails to capture differences in cultural norms (e.g., differences in antibiotic prescribing philosophies/practices)
- Data that does not reflect epidemiological differences among different demographics (e.g., data biased by entrenched over-diagnosis of schizophrenia in African Americans)
- Data encompassing too few individuals with a given demographic (e.g., use of data primarily on older, white men to make predictions regarding young native-Alaskan women)
- Data slanted by historical content
- Data skewed toward meeting specified cost metrics may not take into account other information needed to achieve better health care.

Privacy and Security

Myriad of U.S. Laws and Standards

- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**
  - Amended by the Health Information Technology for Economic and Clinical Health Act (HITECH)
- **Other Federal Laws**
  - Federal Alcohol and Drug Abuse Confidentiality Law
  - Children's Online Privacy Protection Act (COPPA)
  - Genetic Information Non-Discrimination Act (GINA)
  - Federal Trade Commission Act (FTC)
  - Gramm-Leach-Bliley Act (GLBA)
  - Fair Credit Reporting Act (FCRA)
  - Telephone Consumer Protection Act (TCPA)
- **State Mental/Behavioral Health, Substance Abuse, Genetic Testing/Counseling)**
- **Other State Laws**
  - Constitutional Right of Privacy
  - State statutes and regulations protecting confidentiality of general health information
  - State statutes and regulations protecting confidentiality of sensitive categories of personal health information (e.g., HIV/AIDS,
  - State Data Breach Notification Laws
  - State Data Disposal Laws
  - State Consumer Protection Laws
  - Common Law Case Law
- **Industry Standards Developed to Promote Self-Regulation, such as:**
  - Payment Card Industry Security Standards Council
  - Mobile Medical Marketing Association
  - National Telecommunications and Information Administration

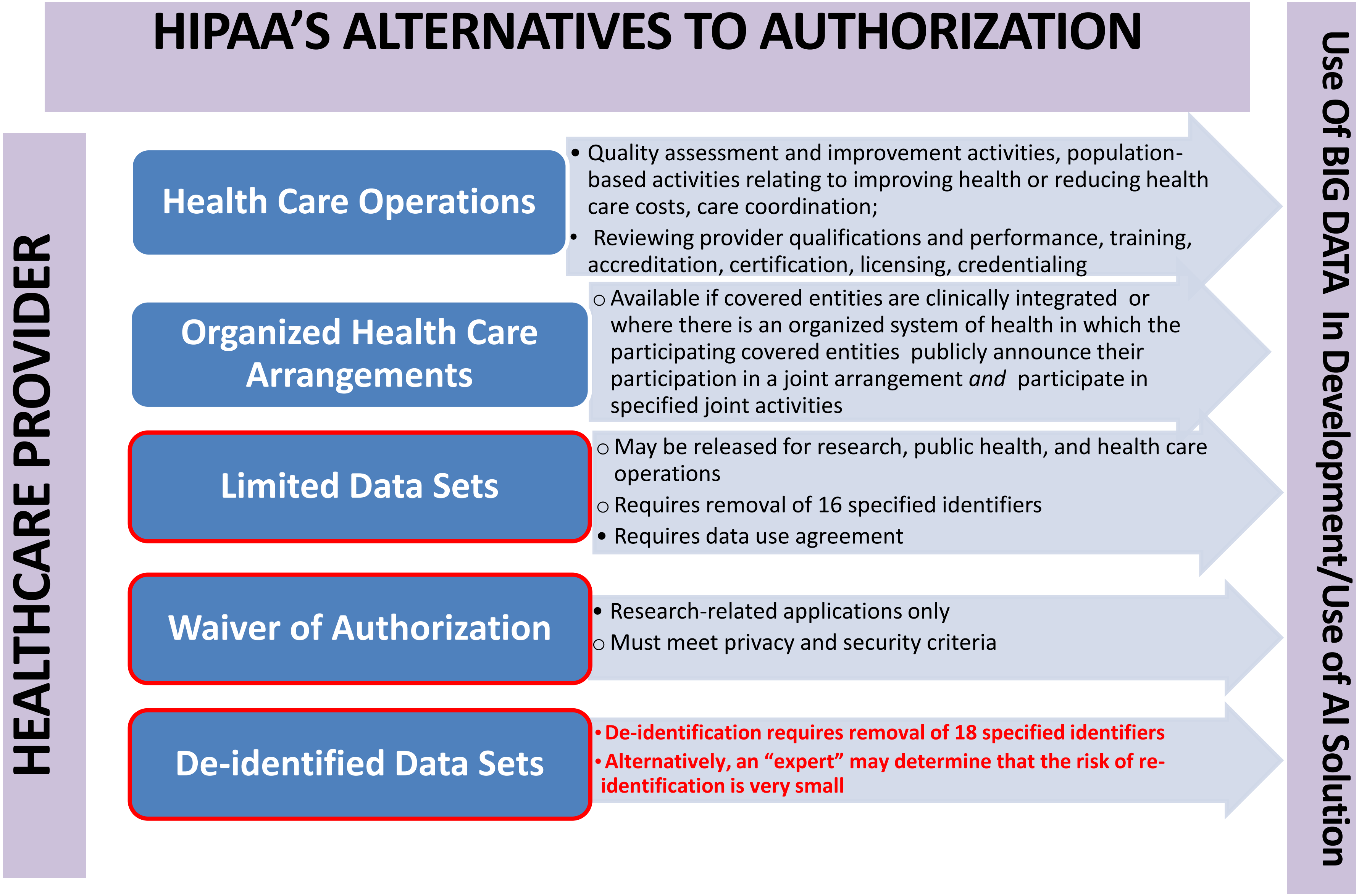
Privacy and Security Risk

"Secondary Use" of Big Data

- Different compliance moments create "Traps for the Unwary"
  - Initial collection/use of PHI for clinical care or research
  - Secondary use of PHI
- Use of PHI for research is research under HIPAA even if used by the CE.
- Use of PHI to build a repository to be used for future research is research
- Lines between "Research" for "Health Care Operations" can be blurry and gray
  - BAA is not a compliance pathway for research activities – not a covered function.
  - BAA is a valid pathway for pure data de-identification of data to support the research if certain requirements are met by the BAA
  - Whether **FDA approval/oversight** is needed is not always determinative.
- Need for IRB involvement?
  - Traditional Review v. Novel Issues (e.g., is it HCO or Research)
  - External IRB v. AMC/University
  - Relative Roles

Privacy and Security Risk

"Secondary Use" of Big Data



HIPAA'S ALTERNATIVES TO AUTHORIZATION

HEALTHCARE PROVIDER

Health Care Operations

- Quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, care coordination;
- Reviewing provider qualifications and performance, training, accreditation, certification, licensing, credentialing

Organized Health Care Arrangements

- ○ Available if covered entities are clinically integrated or where there is an organized system of health in which the participating covered entities publicly announce their participation in a joint arrangement *and* participate in specified joint activities

Limited Data Sets

- ○ May be released for research, public health, and health care operations
- ○ Requires removal of 16 specified identifiers
- Requires data use agreement

Waiver of Authorization

- Research-related applications only
- ○ Must meet privacy and security criteria

De-identified Data Sets

- **De-identification requires removal of 18 specified identifiers**
- **Alternatively, an "expert" may determine that the risk of re-identification is very small**

Use Of BIG DATA In Development/Use of AI Solution

Secondary Use of Big Data

HIPAA Sale of Data Prohibition and De-Identification Challenges

- **HIPAA Sale of Data Prohibition Requires Patient Authorization or De-Identification of Data**
  - No “remuneration” for PHI other than reimbursement of costs incurred to transmit and collect
  - Limit on “remuneration” does not apply to sale/license of **De-Identified Data**
  - **Limited Data Set** ≠ De-Identified Data
- **De-Identification Pathway is the likely pathway for avoiding violation of the prohibition.**

Secondary Use of Big Data

HIPAA Sale of Data Prohibition - De-Identification Challenges

- **De-Identification Methods and Challenges**

  The "Black Box" dimension of AI Algorithms exacerbates the de-identification challenge that already exists in any Innovation Strategy driven by Big Data.

  – **Safe Harbor – Removal of 18 identifiers may be inadequate in AI Contexts**

    - Risk of re-identification becomes greater when data that was de-identified under the "Safe Harbor" is combined with myriad other data not created or controlled by the covered entity
    - Covered Entity will have difficulty demonstrating that it **has no actual knowledge that the data remaining after the de-identification process "could be used (alone or in combination with other information) to identify** an individual who is the subject of the information."

  – **Statistical Certification method is increasingly being considered necessary**.

    - AI presents a "New Horizon" for many certification experts
    - Pool of qualified experts is lacking.

Secondary Use of Big Data

Inconsistent De-Identification Standards

- Applicable Laws **lack consistent standards for de-identification** of individually identifiable information
- HIPAA's Safe Harbor de-identification method is the most precise, but may not satisfy GDPR standard for "anonymization"
- GDPR Determines "identifiability" using a facts and circumstances test based on "all the means reasonably likely to be used … either by the controller or another person to identify the natural person directly or indirectly"
  - Key-coded data is generally considered **"pseudonymized"** personal data, **not "anonymized"** and still subject to many of GDPR's protections
  - "Personal Data" include Information that is not "Personal Data" **but that could become so if used with correlating information**

STATE BILLS REGARDING SALE OF DE-IDENTIFIED HEALTH INFORMATION

A number of states have either introduced or indicated plans to propose bills that restrict the sale of de-identified health information

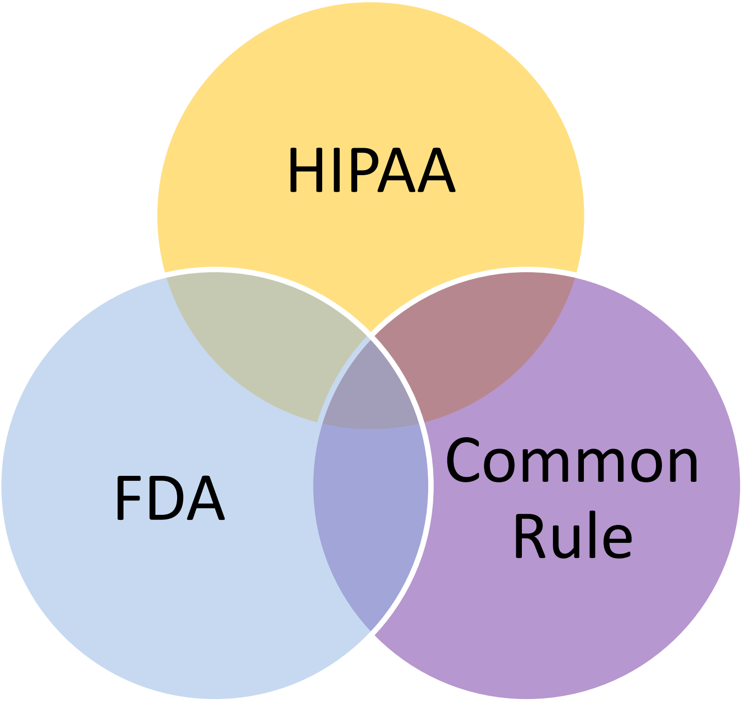
Oregon S.B. 703	Maryland HB892	California: "Data Dividend" Concept
(In Committee)	(Withdrawn 4/5/19)	(Gov. Newsom Proposed in 2/19)

- Oregon and Maryland bills were similar and would require individual authorization before engaging in "commercial sale" of data that is de-identified under HIPAA. Opposition included medical device industry and ACLU.
- The proposals demonstrate an increased sensitivity to secondary use and the need for both the sources and recipients of data for secondary use to have a clear compliance framework for secondary use and to consider patient and public relations issues.

Secondary Use of Big Data

HIPAA v. Common Rule v. FDA Research Regulations

- HIPAA, Common Rule and FDA Research Regulations are **now more fully harmonized** with regard to whether consent/authorization is required for secondary use.
- **Some inconsistencies remain**:
  - ***Common rule*** permits use of ***broad consent*** to secondary use for research (but no IRB waiver will be allowed if subject declines to provide broad consent)
  - ***Potential misalignment with HIPAA* authorization** which may require more specificity than broad Common Rule consent.
  - ***Not aligned with FDA***, which has no consent exemption for use of de-identified information (except for certain IVD investigations), not even for a Limited Data Set
  - ***New Common Rule Exemption*** for HIPAA compliance applies **only** to **Use** and **not** **Disclosure**.



Secondary Use of Biospecimens

McDermott Will & Emery

- Common Rule ANPR and NPR:
  - ***proposed that biospecimen – even if otherwise non-identifiable under HIPAA – would be considered a "human subject".***
  - Not included in Final Common Rule.
- **BUT: Final Common Rule mandate for periodic reassessment of this issue creates a Specter for the future use of AI Software in Precision Medicine Applications**

Data Privacy and Integrity Risk

Due Diligence of Data Sources

- Conduct **due diligence and monitoring** to assess the right of any **source from which data is received** has to collect and share the data.
  - What was the source of the data?
  - What regulatory pathway applied to the original collection of the data? To the subsequent sharing and use?
  - **Who was responsible for complying** and **did they comply**, **at each juncture** in the flow of the data? Was compliance strategy fully implemented and enforced?
  - How do the compliance steps taken at each juncture along the way affect the compliance strategy and risk at **each subsequent juncture**?
    - Tracking of consents/refusal or withdrawal of consents and any special restrictions imposed
    - Tracking of disclosures and promises made in notices and privacy policies
- **Challenges will arise in finding out what prior steps were taken.**
- **This is also helpful for assessing DATA INTEGRITY**

Data Risks and Challenges
Contracting with Data Sources

- Contractually require third parties from whom you **obtain** **d**ata to represent and warrant regulatory compliance and best practices.
- Contractually require third parties with whom you **share** data to:
  - Use the data consistently with the third party's assurances (e.g. no new or additional uses that were not contemplated at the time the data was shared),
  - Safeguard the privacy and security of the data,
  - Report security incidents and breaches,
  - Otherwise comply with all applicable legal and regulatory requirements.
- Contractually require third parties from whom you **obtain** data to represent and warrant accuracy and completeness of the data.

Big Data Privacy and Security

Cybersecurity Risk

- Data collection, aggregation and transmission in support of AI Innovation occurs in an environment that may be far less controllable than the traditional EHR.
- **This exponentially exacerbates risk of breach and cyberattack.**

> ***One of the security challenges for Big Data platforms is inherent in their design. Unlike transaction information systems, analytic systems are intentionally designed to allow for large amounts of data to be pulled out easily in one query. As a result, traditional auditing and intrusion detection methods are not effective, for both external and internal attacks.***

Dale Sanders, Executive VP for Product Development Health Catalyst

Emerging FDA Framework

Useful Guideposts

- The 21st Century Cures Act requires that exempted CDSS **must allow a "health care professional to independently review the basis for its recommendations** so that it is not the [manufacturer's) intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.“
  - FDA's draft CDS guidance states that rules-based AI could meet this standard by using publicly available clinical practice guidelines, published literature, FDA-approved labels, etc., but did not explain what the standards might be for data-based AI.
- Cures Act allows FDA to **override** Cures Act’s exclusions of software from “medical device” definition if the software at issue:
  - Would present a **significant likelihood and severity of patient harm** if it does not perform as intended; **or**
  - Is likely to **supplant rather than support the clinical judgment** of the user taking into account whether the user has the opportunity to independently review the basis of the decision as well as the intended user and use environment.

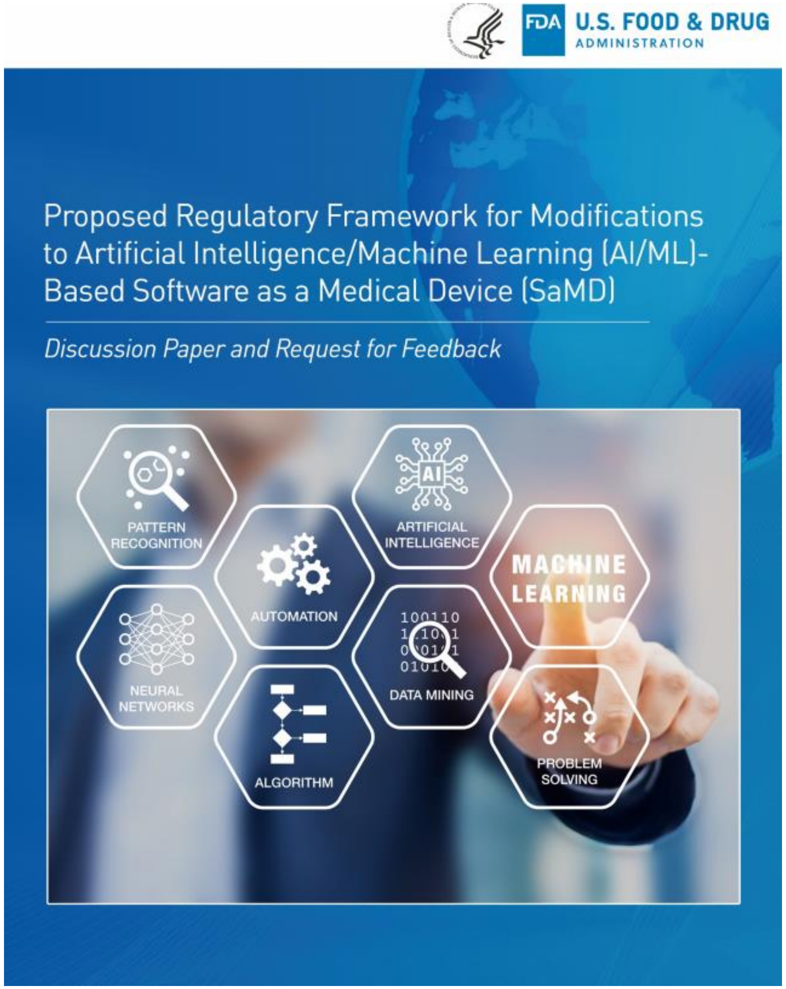
Emerging FDA Framework

Useful Guideposts

- ***Likelihood the FDA will exercise the override authority and subject the AI to full pre-market increases as:***
  - ***AI technology comes closer to highly sophisticated "black box" technology that does not enable independent clinician review of the basis for the recommendation or solution, and***
  - ***AI-generated recommendations come closer to being the primary or sole basis for a diagnosis or treatment.***

Emerging FDA Framework
Useful Guideposts

- FDA exploratory paper outlining a proposed regulatory framework for AI/ML-based software products that could achieve a substantial shift in FDA oversight (April 2019)
  - Proposes a “**Total Product Life Cycle**” (TPLC) approach to modifications.
  - Highlights the “**Spectrum of Dynamism**” and complexity of AI as a key factor in developing the right model.



FDA U.S. FOOD & DRUG ADMINISTRATION

Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)

Discussion Paper and Request for Feedback

Emerging FDA Framework
Useful Guideposts

- **Potential for Modifications over the Total Product Life Cycle**
  - FDA anticipates that many (although not all) modifications to AI/ML software over its Life Cycle will involve "**algorithm architecture modifications and re-training with new data sets**," which would be subject to premarket review.
- Categories of modifications:

  (1) **Performance,** which modify clinical and analytical performance,

  (2) **Inputs,** which are used by the algorithm and their clinical association with the SaMD output, or

  (3) **Intended use**, which is described through the significance of information provided by the SaMD for the state of the healthcare situation or condition.

Emerging FDA Framework
Useful Guideposts

- **"Spectrum of Dynamism"**
  - A "**Locked Algorithm**" is less complex and provides the same result each time for the same input.

    FDA has only approved AI using locked algorithms

  - **A "Continuously Learning Algorithm"** adapts and changes its behavior using a defined learning process. For a given set of inputs, the output may be different before and after the changes are implemented via AI/ML processes.

  FDA has not yet approved AI using a continuous learning algorithm.

Emerging FDA Framework
Useful Guideposts

McDermott Will & Emery

4 GENERAL PRINCIPLES TO BALANCE BENEFITS AND RISKS OF AI/ML-BASED MEDICAL DEVICE

- Establishing clear expectations on **quality systems and good ML practices (GMLP)**
- Conducting premarket review for AI that requires premarket submission to **demonstrate reasonable assurance of safety and effectiveness** and establishing clear expectations for manufacturers of AI/ML-based SaMD to manage patient risks throughout the lifecycle of the software (i.e., relying on the principle of a "**predetermined change control plan**" that anticipates certain modifications, the "SaMD Pre-Specifications," and associated methodology for those changes, the "Algorithm Change Protocol" in a controlled manner that manages risks to patients)
- Expecting manufacturers to perform **continuous monitoring** on their AI/ML devices and incorporate a risk management approach and other approaches outlined in FDA's "Deciding When to Submit a 510(k) for a Software Change to an Existing Device" guidance in the development, validation, and execution of the algorithm changes
- Enabling increased transparency to users and FDA using **post-market real-world performance reporting** for maintaining continued assurance of safety and effectiveness

Emerging FDA Framework

Transparency And Real-world Performance Monitoring

- Appropriate mechanism will vary and may include:
  - Periodic reporting to FDA, collaborators, and public on updates that were implemented and performance metrics
  - Ensuring labeling changes accurately describe modifications and rationale for modifications
  - Updating specifications or compatibility of impacted supporting devices, components, or accessories
  - Establishing procedures to notify users of updates and determining what information could be provided

Malpractice Liability

- **AI is Uncharted territory** – no known case law to date
- AI Software by its nature creates challenges in applying long-standing legal tenets such as **human causation** and **foreseeability** for assessing, managing and allocating malpractice risk and liability.
- **Potentially greater risk that AI error in judgment will be replicated across a greater number of patients then a Human error in judgment.**
- **Key Factor: Where does the AI fall on the "Spectrum of Dynamism"**
  - Locked v. Continuous Learning v. General AI/Black Box
- **Key Factor: Where is the AI in its Total Product Life Cycle?**
  - How will it be modified over time?
  - Is there a plan for subsequent changes and how will quality be re-tested and re-validated?

Malpractice Liability

Coping with the Ambiguity in the Law

- **Key Considerations**
  - Does the AI present a significant likelihood and severity of patient harm if it does not perform as intended?
  - Who is the intended user (clinician/patient)?
  - What is the intended use environment?
  - Is the AI likely to supplant rather than support the user's clinical judgment?
  - Will the user have the opportunity to independently review the basis of the AI software's decision/recommendation?

The closer the AI Algorithm comes to the "black box" end of the Spectrum the more challenging becomes the assessment, management and allocation of malpractice risk.

QUERY: **Will greater FDA scrutiny of an AI Solution reduce malpractice risk?**

Malpractice Liability

Causation

- Various players are involved in the development and use of the AI technology, they play different roles and make different contributions:
  - Developers and manufacturers
  - Vendors who sell, implement and maintain the technology
  - Purchasers (e.g., health systems, physicians)
  - Physicians and other Clinicians who:
    - Train the AI Solution or develop the Rules and/or datasets used to train it
    - Oversee the use of the AI Solution
    - Rely on the AI solution to support/make diagnosis and treatment recommendations/decisions
  - Patients

QUERY: Will the AI Software itself take on "Personhood"?

Malpractice Liability

Causation and Forseeability

- Departure from long-standing norms of traditional roles and relationships of physician and patients
- Patients may assume some of the risk as a result of increased engagement in and control over their health and health information through digital health tools and mobile devices.
  - Physicians may be working in part with data, AI tools and diagnostic information from AI tools chosen, created and maintained by the patient and not the physician
- **QUERY:** *How can/should the analysis of **foreseeability** take into account the fact that some AI machine learning is designed to find connections and patterns within data and images that humans cannot?*

Malpractice Liability
Changes in the Standard of Care

- **Will AI elevate or otherwise change the standard of care?**
  - Will a court expect practitioners to take advantage of available AI diagnostic and treatment solutions?
  - If so, to what extent.
  - If not now, when?
  - On whose **expert testimony** will the court rely to determine whether the right decision was made concerning whether to use AI and whether the right decision was made when using it?
    - Other physicians
    - Computer programmers or engineers
    - Data Analysts
    - The AI Software itself
    - Some combination thereof?

Malpractice Liability

Changes in the Standard of Care

- What **evidence of safety and effectiveness** will be sufficient to warrant inclusion of AI solutions in the standard of care?
  - Changes to Standard of Care normally require robust peer-reviewed research, testing and validation.
- Changes in the Standard of Care will have a ripple effect into **insurance coverage** strategies and approaches and the overall economics of health care.

Product Liability

- **Strict Product Liability** actions may arise from an unreasonably dangerous defect or design, manufacture or labeling of the product that produces an actionable injury.
  - Black Box nature of AI Software may make it difficult to identify/prove a defect (or lack thereof)
- **Breach of Warranty** actions may arise from sale of product to a consumer that is not a reasonable fit for the purposes or intended use for which it was sold.
- AI manufacturers may call on the **"Learned Intermediary"** doctrine to shift liability to physician who developed training rules, designed testing data, and/or based medical decision on AI input.
  - Aggressive direct-to-consumer marketing has eroded the strength of this doctrine.
  - Direct-to-consumer marketing of AI Software may be less likely than with other healthcare products such as drugs.
  - Again, **"Black Box" nature of the AI Software** may undermine reliance on this doctrine.

Transparency / Fraud and Deception

Consent Practices

- **When is it necessary to specifically call out and to explain the use of AI in diagnosis and treatment decisions?** Will that depend on:
  - The nature of the AI
  - The nature/severity of the health care disease/condition for which it will be used?
  - The extent to which the practitioner will rely on the AI to support the medical judgment?
  - The extent to which the practitioner can explain/understand how the AI arrived at the outcome/recommendation (particularly when the AI is a Neural Network)?
- How to achieve **understandability** and **explainability** for the patient of a complex technology solution that providers themselves may not understand?
- Whether to give the patient the opportunity:
  - to **refuse to allow use of AI** in diagnosis or treatment, or
  - To **reject a diagnosis or treatment plan** based in whole or in part on the use of AI?

Transparency / Fraud and Deception

Consent Practices

- Manufacturer privacy notice and terms of use may not be enough or apply at all
- Anticipate **layers of consents** and notices given at different points in time by various stakeholders involved in the life cycle
  - Notice/consent "**Just in Time**" prior to data collection
  - Need for Consistency and Coordination among consents at the various layers
- **Anticipate need to review and revise notices and consents periodically to adapt to changes** in AI functionality, use, disclosure, quality and safety risks, privacy and security infrastructure etc.

Risk Oversight and Management

- **Compliance Program**
  - Current Compliance Programs should integrate current and emerging AI Innovation compliance risk considerations into the compliance program if not currently addressed.
  - Combination of enhancements to existing policies and procedures and addition of new policies and procedures.
- **Contractual Risk Management and Allocation**
  - Affirmative Covenants
    - Privacy and Security Infrastructure
    - Data Integrity
    - Overall Legal and Regulatory Compliance (FDA, Privacy/Security, Consent/Transparency)
    - Truth in Advertising
  - Allocation of Compliance and Liability risk
    - Product safety v. Medical decision-making
    - Indemnification
    - Liability disclaimers and limitations/caps
    - Corresponding Insurance

Risk Oversight and Management

WORD TO THE WISE:

Contractual allocation/shifting of risk is NO SUBSTITUTE for pre-contracting due diligence.

McDermott
Will & Emery

Potential Data Privacy and AI Risks in the Product Life Cycle of a Medical Device

Bernadette M. Broccolo
Partner
McDermott Will & Emery LLP
312.984.6911
bbroccolo@mwe.com