****

The Evolving Ethical and Legal Framework for the Use of Artificial Intelligence in the Pharmaceutical and Medical Device Industries

*June 2020*

Contents

[Overview 3](#_Toc42611937)

[What is Artificial Intelligence? 3](#_Toc42611938)

[How Are Pharmaceutical & Medical Device Companies Using AI? 4](#_Toc42611939)

[Research and Development Case Study: Identifying Drug Targets 5](#_Toc42611940)

[Clinical Trials Case Studies: Optimizing Clinical Trial Design and Conduct 5](#_Toc42611941)

[Diagnostic Case Study: Using AI and Medical Imaging For Early Diagnosis 6](#_Toc42611942)

[The Evolving Ethical and Legal Framework for the Use of AI 7](#_Toc42611943)

[Established Principles and Guidelines for the Use of AI 8](#_Toc42611944)

[Practical Considerations for the Ethical Use of AI 9](#_Toc42611945)

[Fairness 9](#_Toc42611946)

[Transparency and Explainability 10](#_Toc42611947)

[Accountability 10](#_Toc42611948)

[Data Privacy and Security 11](#_Toc42611949)

[Appendix: GLobal & Regional Principles and frameworks 18](#_Toc42611950)

[REFERENCES 22](#_Toc42611951)

Copyright © 2020 International Pharmaceutical and Medical Device Privacy Consortium

All rights reserved.

# Overview

Artificial intelligence is revolutionizing the ways in which we use, interpret, and understand data. AI’s power stems from its ability to rapidly analyze data and identify patterns, and applications of AI are quickly changing the way that work is done globally. The potential of AI is especially significant within the pharmaceutical and medical device industries, where it holds promise for accelerating research and development and improving our ability to effectively diagnose and treat patients. However, the use of AI also presents a host of new ethical concerns. In response, lawmakers, standards organizations, trade associations, and other entities are developing new ethical and legal frameworks that apply to AI.

This IPMPC white paper presents an overview of emerging uses of AI within the pharmaceutical and medical device industries, along with commentary on the emerging ethical and legal frameworks for AI and practical considerations for use of AI.

# What is Artificial Intelligence?

**Artificial Intelligence**, commonly known as “AI,” has generally included research areas like reasoning, knowledge representation, planning, learning, natural language processing, perception and visualization. Approaches include statistical methods, computational intelligence, and traditional symbolic AI. Many tools are used in AI, including versions of search and mathematical optimization, artificial neural networks, and methods based on statistics, probability and data science. The AI field draws upon computer science, information engineering, mathematics, psychology, linguistics, philosophy, and many other fields. Experts in AI appropriately assert that AI and Machine Learning (ML) are different disciplines. However, in much that is written and presented, both in general media and among technologists, the terms AI and ML are often used interchangeably.

A common Machine Learning (ML) use case encompasses software that uses and analyzes data to improve its underlying analytical capabilities, often called a model. This ML model is created and includes algorithms, with data, and a human step to validate that the model is providing accurate or valid results. This validation step is called training. ML models in place are “trained.” (Retraining of these models is very application dependent – some are retrained with new data very frequently; some models are unchanged for months or even years.)

There are several categories of AI/ML that have seen very rapid increase and are being applied to clinical data and medical devices (like most industries).

* **Supervised Learning** uses well-defined (labeled) input data for its computation and are trained to look for expected patterns in the data. The algorithms are implemented in software and are trained in a close looped process with data, software, analysis, and human validation. When the desired threshold of accuracy is achieved, these trained models are deployed. The trained, deployed model (software) accepts and then processes/analyzes the input data and provides the results. Google Search, the Netflix recommendation system and most spam email detection systems are examples of supervised learning ML applications.



**Training Data** applied to the model / algorithm, creating a result (prediction) that is evaluated. When satisfactory results status is reached, the trained model is deployed. **Input Data** is then fed into the model / algorithm, and used in “production.” Retraining life cycles vary.

Use

blogs.teradata.com

 Figure 1: Training Data

* **Unsupervised Learning** uses self-learning techniques where the system is expected to discover the features or patterns that may exist in the data. Clustering and association techniques are common methods of unsupervised learning. The most frequently cited use of unsupervised learning is the identification and/or classification of objects, people or animals in image data.
* A third type of system, **Reinforcement Learning**, is another ML paradigm. This model is trained by trying, in software, a variety of paths or means to reach goal, and continuously learning the paths that lead closer to a desired solution and minimizing or excluding the paths that tend away from the desired solution. Smart vacuums and autonomous vehicles are prominent examples of systems that use reinforcement learning.
* Supervised Learning is the dominant method for Machine Learning today. But within these 3 major areas of ML, several subdomains are growing rapidly. Techniques or methods that are prominent in academia, the tech companies and in the data science communities include: Time-Series analytics, Deep Learning, Convolutional Neural Network (CNN), Generative Adversarial Networks (GANs), Computer Vision (CV), Natural Language Processing (NLP), and Transfer Learning.

# How Are Pharmaceutical & Medical Device Companies Using AI?

AI has numerous applications within the pharmaceutical and medical device industries, and is transforming the way the life sciences sector understands and leverages data. Future technological advances will likely enable AI to play a greater role in drug development. Today, companies are increasingly using AI to, among other things:[[1]](#endnote-1),[[2]](#endnote-2)

* increase the speed and efficiency of drug research and development by identifying patterns in patient records and genetic information;
* identify patient candidates for clinical trials;
* improve adverse event monitoring and reporting; and
* create risk-adjusted population health informatics, and
* develop custom devices, for example prosthetics and orthodontic aligners, and
* analyze data and medical imaging to identify patterns and improve patient diagnoses.

The case studies below describe a variety of ways in which artificial intelligence is being used by pharmaceutical and medical device companies.

### Research and Development Case Study: Identifying Drug Targets

AI helps researchers throughout the drug research and development process. Some examples include discovering biomarkers, developing hypotheses, and identifying targets for potential new drugs.[[3]](#endnote-3) Though these uses are still in preliminary stages of research and use, AI is improving rapidly. The use of AI to identify targets for new drugs appears to be on the horizon. Many life sciences companies, AI vendors, and academic institutions are investing heavily in this type of technology. Researchers affiliated with McGill University, for example, are using AI to analyze MRI scans.[[4]](#endnote-4) Their hope is that the AI system might be able to identify a pattern of anomalies in the scans that human researchers have yet to identify, leading to a new treatment for multiple sclerosis (MS).[[5]](#endnote-5) Similarly, in 2018, the World Economic Forum listed AI for molecular design as one of the top ten emerging technologies.[[6]](#endnote-6) AlphaFold, part of Google’s DeepMind AI program, for example, is using AI to map three-dimensional models of proteins.[[7]](#endnote-7) Understanding how various proteins fold, the company asserts, may help scientists better understand and cure diseases that researchers believe are caused by misfolded proteins – including Alzheimer’s, Parkinson’s, Huntington’s, and cystic fibrosis.[[8]](#endnote-8)

### Clinical Trials Case Studies: Optimizing Clinical Trial Design and Conduct

AI can be applied in context of clinical trials to design future trials, more rapidly identify clinical trial participants and connect patients with clinical trials, and improve clinical trial data, among other uses.

##### Designing Trials

Existing AI tools can analyze a broad range of data on prior clinical trial successes and failures to identify factors that help trials succeed. Designing new clinical trials based on these results helps ensure their success, streamline the clinical trial process, and reduce overall clinical trial costs.[[9]](#endnote-9) Trials.AI, for example, seeks to decrease overall clinical trial costs by mining data to identify factors that promote trial success. The company’s software predicts the best study sites, trial protocols, and participants, among other factors.[[10]](#endnote-10)

##### Identifying Patients

AI systems are helping companies better identify candidates for clinical trials. Many AI companies working in this area have focused on increasing the number of patients in clinical trials, selecting them more efficiently, and supporting patient selection by aggregating data across healthcare providers. Deep 6 AI, for example, recently debuted a system that rapidly identifies patients for clinical trials.[[11]](#endnote-11) In one hour, its system identified 16 pediatric heart surgery candidates for a drug trial.[[12]](#endnote-12) By comparison, the affiliated hospital’s research team took an average of six months to identify two trial candidates.[[13]](#endnote-13) Similarly, Tempus seeks to place more cancer patients in clinical trials. The company built a network of over 40 healthcare providers and analyzed their cancer patient data in the aggregate to match patients with clinical trials via molecular profiling.[[14]](#endnote-14) This has the potential to not only increase clinical trial participation rates but also to offer opportunities to patients who are geographically located in areas with few clinical trials.[[15]](#endnote-15) Other companies are developing AI solutions to sustain subject participation in trials. Brite Health, for example, is doing so by analyzing data to predict which clinical patients are at risk of non-adherence and/or dropping out.[[16]](#endnote-16)

##### Improving Clinical Trial Data

Having standardized, high-quality patient data is essential when conducting clinical trials and analyzing trial data. While companies provide standardized case report forms to clinical trial sites to ensure that data is collected in a structured manner, information about patients is often also captured in clinical notes. Abstracting useful information from these notes and converting it into structured information that can be used in analysis can be time-consuming, requiring careful review by trained professionals. Natural language processing (NLP), one form of AI, helps to address this by reading clinical notes more quickly and efficiently than a human could. With this technology, the clinical notes can then be converted into usable data (e.g. by populating structured fields with the information read from the notes) that can be analyzed with machine learning systems to identify patterns and help researchers better understand clinical trial results.[[17]](#endnote-17)

### Diagnostic Case Study: Using AI and Medical Imaging For Early Diagnosis

AI also has the potential to improve diagnostic capabilities, which may lead to more rapid intervention and possibly improve patient outcomes. Tele-radiology has existed for more than 20 years. Now companies are using AI to review MR, CT, XR and other diagnostic images After being trained with large numbers of images, the systems can be used to identify abnormalities or changes in a patient’s imaging to help physicians efficiently diagnose medical conditions. In 2016, for example, Google Brain demonstrated that one of its AI programs could, after analyzing over 120,000 images of human retinas, diagnose diabetic retinopathy with the same level of accuracy as a doctor.[[18]](#endnote-18) Early detection of the disease aided by this technology, Google asserts, may help provide early and effective treatment to limit permanent blindness.[[19]](#endnote-19) Similarly, researchers at UCLA developed a system called FocalNet, which analyzes MRI results to identify prostate cancer. In testing the system’s effectiveness, UCLA found that radiologists with ten years of experience were 83.9 percent accurate in their diagnoses. In published results, FocalNet, which had been trained with 417 MRI scans, was 80.5 percent accurate.[[20]](#endnote-20)

# The Evolving Ethical and Legal Framework for the Use of AI

While applications of AI hold exciting potential for the pharmaceutical and medical device industries, its use also raises new legal questions and ethical issues. From a legal perspective, one of the fundamental questions that arises is how AI software within life sciences and healthcare settings will be regulated and whether the software itself will be considered a medical device for legislative purposes.[[21]](#endnote-21) From an ethical perspective, myriad questions arise about how to protect the individuals whose data is used and analyzed; how to identify, account for, and prevent bias, which may arise from bias inherent in the data used to train software; and the intent behind artificial intelligence systems, and whether they are being used in an appropriate context and for ethical purposes.[[22]](#endnote-22) Two examples illustrate such ethical issues:

* One example is that of AI software trained on limited data sets that lack representation from certain ethnic groups. When used prospectively, this software will reflect that selection bias, which may compromise the integrity of insights generated by the software and its ability to provide relevant insights for the ethnic groups excluded from the original data set.
* As a second example, it is possible that clinical decision support tools designed to promote a single objective, for example the highest quality healthcare, could be trained to encourage clinical decisions that improve that key quality metric, and inherently suboptimize other aspects of care. The AI system could promote prescription of certain drugs or bias to therapies that are inconsistent with care availability, family constraints, etc.

As AI becomes more widely used, it is essential that issues such as these are identified and addressed. Awareness of this need has driven multi-national bodies and regional governments to define guidelines and laws to govern the use of AI. The remainder of this paper will focus on this evolving framework, emphasizing key principles, guidelines, and laws relevant to AI along with practical considerations for adhering to these principles, guidelines, and laws.

As the medical device and pharmaceutical industry rapidly adopt AI systems to aid in trials, research and new product development, the use and governance of the data in these systems poses new challenges. Several technologies and imperatives are exposing a number of practical needs for attention:

* Advanced analytics capabilities are available to almost all functions in healthcare (and other) companies today. Many are beginning to have built-in AI capability. This “low barrier to use” this data requires much broader compliance programs in general. Coming soon is the ability for non-technical staff to build and train their own AI models.
* Training of AI models is inherently a data aggregation process. Thoughtful consideration must be given to the economics and logistics of retraining models if the exclusion of some subset of the data is required. (In other words, a model cannot be untrained by removing a subset of the data without full retraining, in the same way one cannot take half the eggs out of a baked cake.)

Explainable AI is a fast growing research field in AI. Human-understandable evidence that can articulate WHY the AI model arrived at its results is a desired and often required element of AI systems. Especially in healthcare and other new spaces. Many readily accept Amazon and Netflix recommendations without knowing how or why. The same cannot be said for treatment plan recommendations or predictive analytics about individuals’ health. The power of AI to look at thousands of factors in millions of health records and find heretofore unseen correlations has great promise, but without human explainability, this poses numerous challenges to researchers, companies and regulators.

## Established Principles and Guidelines for the Use of AI

Several multinational organizations have provided guidance on principles, guidelines, and best practices to underpin the use of AI within business, research, and other areas. Common themes transcend these guidelines, and, taken together, they provide a framework to guide adoption and use of AI. The main guidelines from multinational organizations are:

* OECD: Principles on Artificial Intelligence
* European Commission: “Ethical Guidelines fo Trustworthy AI”
* International Panel on AI (IPAI): Ten
* United Nations Educational, Scientific and Cultural Organization (UNESCO): ROAM Principles
* Council of Europe: “Guidance on Artificial Intelligence and Data Protection”
* canada’s Office of the Privacy Commissioner: Proposals

Descriptions of the above guidelines can be found in the Appendix at the end of the document.

## Practical Considerations for the Ethical Use of AI

Although non-binding, the guidelines listed above have garnered substantial international support. Even as the legal framework for AI continues to develop, life sciences companies may want to consider how these guidelines relate to their current usage of AI technologies and whether adjustments may be needed to promote adherence to the principles that transcend these guidelines, including the protection of key values, including fairness, accountability, transparency, and data privacy and security. This final section of this paper presents practical considerations for adherence to these principles.

Figure 2: Key Values to Promote Ethical Use of AI

### Fairness

Guidelines regarding the ethical use of AI focus on fairness in two ways. First, they assert that AI users must ensure equal access to AI technologies across population groups of different ages, races, ethnicities, genders, socio-economic statuses, etc. Second, they seek to ensure that AI systems are trained without bias. AI systems may have bias (or become biased) for a number of reasons: poor (biased) data, bias inherent in the algorithms (underlying mathematics, statistics or software), researcher bias, etc. AI systems inherently adopt the tendencies and biases of the data on which they are trained.[[23]](#endnote-23) Having no ability to truly “think” on their own, they merely learn and repeat whichever biases exist in that data. Therefore, AI systems are more likely to reflect biases when they have been trained only on a small subset of data. Systems trained with data from only one medical facility, for example, will reflect the decision-making tendencies of that facility’s doctors.[[24]](#endnote-24) Similarly, systems trained on data sets that lack ethnic diversity will not be able to account for variances in genetics and disease risk across ethnicities. These types of biases can compromise the validity of AI predictions and prevent certain population groups from benefiting from AI.

Companies may wish to consider the ways in which their current use of AI promotes any biases – explicit or implicit – and evaluate whether changes to their current processes would provide more equal access to treatments to their patients and prospective patients. Utilizing large data sets with data points representing broad range of population groups can help achieve this goal.[[25]](#endnote-25) Companies may want to consider whether sharing data with other pharmaceutical and medical device companies for the purposes of training AI systems on sufficiently large and broad data sets would be beneficial. One such data sharing agreement was launched earlier this year – ten pharmaceutical companies agreed to share their data with AI start-up Owkin in order to train the company’s algorithms and increase the speed of drug development.[[26]](#endnote-26)

Finally, to the extent that certain AI systems are intentionally trained only on data applicable to a certain sector of the population, companies may want to consider implementing internal controls to ensure that those systems are only used to analyze data from individuals who properly fall within that group. This will help avoid the use of AI systems in a way that could provide inaccurate or even harmful predictions.

### Transparency and Explainability

Guidelines regarding the ethical use of AI also highlight the importance of allowing individuals who interact with AI systems and about whom decisions are made by AI systems the opportunity to understand how the system is affecting them.

Companies should determine whether, when, and how to disclose their use of AI systems. Since AI systems are inherently complex, crafting a digestible explanation of the AI and its application may become a difficult undertaking. Companies will also want to decide what information should be included in these disclosures. The OECD’s principles suggest that individuals should be given enough information to allow them to challenge the results it produced by an AI. It may not be feasible nor desirable to provide prospective patients with in-depth details demonstrating how an AI algorithm works. Companies could consider whether providing basic information about AI algorithms that may help improve patient confidence in the system’s treatment recommendations. However, given the inherent complexity of AI systems providing such basic information in an easily understandable manner may prove difficult.

Companies must improve their internal tracking of AI systems, the data that comprises the systems, and the AI operational life cycle. It includes but is not limited to: clear records detailing all AI systems in use, data included in training, reproducible software and algorithms of the AI systems. It may also include internal explainability process– methods whereby employees are able to sufficiently understand the AI algorithms and capabilities of the AI systems, including the basic understanding of its process steps in context.

Having a strong internal understanding of how AI systems work may help companies protect their investment in AI by 1) allowing them to ensure that AI systems are functioning properly and being corrected as needed and 2) permitting companies to defend their algorithms’ results if called into question.

### Accountability

AI algorithms that are properly trained, used, and monitored have been shown to have lower error rates than humans in many instances. They can also consider significantly more data in making their predictions. On the other, flaws in an AI system’s design, updates, use, or data integrity could have substantial negative consequences. This could result in the systematic recommendation of improper patient diagnoses or treatments, invalid analysis of medical images or healthcare predictions based on biased or unsound data. Guidelines regarding the ethical use of AI suggest that companies should be accountable for the failure of their AI systems.

### Data Privacy and Security

To make accurate predictions about the data they analyze, AI systems are often trained on large data sets. Technologically, more data generally leads to more accurate results. However, training the AI systems with large quantities of real patient data raises multiple privacy issues. Guidelines regarding the ethical use of AI consistently include data privacy and security as key. Using patient data in AI algorithms also implicates requirements of Europe’s General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA). Companies must comply with these legal requirements in all uses of AI technologies. Further, companies should consider whether going beyond the strict terms of these requirements better supports the use of an “ethical AI.” This section outlines the key privacy concerns relevant to developing and utilizing AI technologies.

##### Training AI Systems

Using anonymized data when training AI algorithms can limit compliance concerns, but may be difficult to achieve. Anonymized data generally isn’t considered personal data, and does not trigger various rights and obligations under the GDPR, CCPA, and HIPAA.[[27]](#endnote-27) Once data has been anonymized, companies should not maintain a key or other information that would permit re-identification of the personal data. Neither the GDPR, CCPA, nor HIPAA require companies to be able to re-identify data that has been anonymized in order to comply with their other provisions.[[28]](#endnote-28)

To the extent companies do not or cannot anonymize personal data before using it to train an AI algorithm, such processing will fall under the requirements of the GDPR, CCPA, and HIPAA. This includes using key-coded data, which can be re-identified if the key is available .[[29]](#endnote-29) Some of the main requirements are outlined below:

GDPR Compliance

To comply with the GDPR, companies must have a legal basis for the processing.[[30]](#endnote-30) Companies should consider which of the bases articulated in GDPR Article 6 applies. The likely potential bases include 1) consent and 2) processing necessary for the legitimate interests of the controller.[[31]](#endnote-31)

To train AI algorithms, companies often use large quantities of existing data. It may not be feasible to obtain consent for this type of processing from thousands of prior patients on which companies have existing records. Moreover, consent can be withdrawn at any time, in which case the research activities carried out with the individual’s personal data must cease. Therefore, companies may want to consider whether their processing to train AI algorithms falls within the legitimate interests legal basis for processing.[[32]](#endnote-32)

Further, when companies use non-anonymized personal data to train AI algorithms, they must consider the impact of other GDPR provisions that remain applicable, such as the rights of data subjects of access, erasure, data portability, objection, and restriction from processing.

When using non-anonymized data, companies should also be mindful of the GDPR’s prohibition on processing of special categories of personal data.[[33]](#endnote-33) Among others, these “special categories” include data revealing racial or ethnic origin, genetic data, biometric data, and data concerning health. GDPR Article 9(2) provides several exceptions to this prohibition. When training AI algorithms in the research context, the appropriate derogation under Article 9 for processing operations involving special categories of personal data could be “scientific ... purposes in accordance with Article 89(1) based on Union or Member State law.” [Article 9(2)(j); EPDP Opinion 3/2019.]

However, in some instances, companies may not require a new legal basis to process previously-collected personal data for purposes of training AI algorithms, and instead may be able to rely on the legal bases used to collect and process the data initially. Processing of personal data for purposes other than those for which the personal data was initially collected is permitted where the new processing is compatible with the purposes for which the personal data was initially collected. [GDPR Art. 5(1)B).] In such a case, no legal basis separate from that which allowed the collection of the personal data is required.

To the extent further processing for purposes of training AI algorithms constitutes scientific or historical research and is performed by companies in accordance with the requirements set forth in GDPR Article 89(1), such further processing may be considered compatible with the original purpose for which the personal data was collected, requiring no separate legal basis. [GDPR Art. 5(1)B); EDPB Opinion 3/2019.]

CCPA CompliancE

Once the CCPA goes into effect, companies must provide California “consumers,” as defined under the Act,[[34]](#endnote-34) with information regarding their collection of personal information before or at the time it is collected.[[35]](#endnote-35) This information must include the categories of personal information collected and the purposes for which such information will be used.[[36]](#endnote-36) Companies may therefore wish to consider including training AI systems as one such purpose on its notices to consumers. Unlike the GDPR, after initial notice of data collection and intended use is provided to the consumer, companies may not “use personal information collected for additional purposes without providing the consumer with notice.”[[37]](#endnote-37)

Further, when companies use non-anonymized personal information to train AI algorithms, they must consider the impact of other CCPA provisions, such as the rights to notice, deletion, transparency concerning disclosure, opt-out of sale of personal information, and not to be subject to discrimination.[[38]](#endnote-38) Companies should also bear in mind that the use of non-anonymized personal information to train AI algorithms could result in liability under the CCPA’s private right of action.[[39]](#endnote-39) The Act grants a private right of action to all California consumers whose “nonencrypted or nonredacted personal information” is breached due to a company’s failure to implement and maintain “reasonable security procedures and practices.”[[40]](#endnote-40)

HIPAA Compliance

In the United States, HIPAA requires companies to obtain informed consent from clinical study participants for the use of their personal health information. This informed consent may permit companies to use participants’ personal health information for future research purposes as long as the potential for such use is “sufficiently describe[d] . . . such that it would be reasonable for the individual to expect that the protected health information could be used or disclosed for such future research.”[[41]](#endnote-41) However, where pharmaceutical and medical device companies seek to use previously-obtained personal health information to train AI algorithms and those patients’ consent forms did not adequately explain the potential for such usage, a new patient consent or, alternately, an Institutional Review Board waiver of consent may be required.

##### Using AI Algorithms for Decision-Making for New Patients

Harnessing the power of AI means using its algorithms to make predictions and decisions in future cases. In the clinical trial context, for example, companies may wish to use an algorithm trained with data from thousands of diabetes patients in order to predict the proper treatment for a current trial patient.

Anonymization may not be possible in this context. That is, the patient data entered into the AI system must be identifiable in order to ensure that each patient receives the proper treatment. Even if this data is key-coded prior to entry into the AI system, key-coded personal data falls within the requirements of the GDPR, CCPA, and HIPAA.

GDPR Compliance

To engage in this type of processing, companies will want to consider which legal basis to rely on under GDPR Article 6 and which derogation to rely on under GDPR Article 9. Companies may wish to rely on consent, or on the basis that such processing is necessary to the performance of a contract with the patient, or necessary for the legitimate interests pursued by the controller and permitted as part of medical care.[[42]](#endnote-42)

Similarly, GDPR Article 22 gives data subjects the right “not to be subject to a decision based solely on automated processing.”[[43]](#endnote-43) Exceptions to this right include the data subject’s “explicit consent” and where such automated processing is “necessary for entering into, or performance of, a contract” between the data subject and controller. Companies should consider whether they wish to rely on one or both of these exceptions when using AI.

Additionally, at the time of collection of personal data from a data subject, GDPR Article 13 requires that data subjects receive detailed notice regarding the collection and use of their data, including the legal justification for processing their data. To the extent that an AI system will be used to make decisions about a patient, companies should consider how best to disclose this in a way that will provide the patient with sufficient and understandable information about the use of his/her data.

Providing adequate notice to data subjects may depend on the functionality of each AI system. To the extent AI systems are designed to “learn” from all data they analyze, including non-anonymized data entered for the purpose of obtaining a prediction regarding a current patient, companies should disclose this to the patient. That is, proper notice under Article 13 likely requires informing and obtaining consent from patients for both the use of their personal data to obtain a prediction from an AI system and the use of their personal data to train an AI system.

Where AI systems automatically use data entered for a prediction to train their algorithms, such use automatically implicates other rights and obligations under the GDPR. These include the rights of access, erasure, data portability, objection, and restriction from processing. It would also potentially require indefinite retention of personal data in the AI algorithm. To prevent this, companies may wish to consider whether there are technical alternatives that would allow their AI systems to make predictions about a data subject’s personal information *without* also “learning” from that information. The same information, once anonymized, could be re-entered into the system for training.

CCPA Compliance

To use AI algorithms to make predictions with California consumers’ personal information, companies will need to provide notice before or at the time of collection.[[44]](#endnote-44) This information must include the categories of personal information collected and the purposes for which such information will be used.[[45]](#endnote-45) Companies must include in this notice an indication that they intend to use the consumer’s information to obtain a prediction from an AI algorithm, and, if applicable, to train an AI algorithm.[[46]](#endnote-46)

HIPAA Compliance

In the United States, companies may use patients’ protected health information both for initial treatment and for future research purposes. HIPAA requires companies to obtain informed consent for the use of their personal health information. Therefore, a patient’s initial consent may authorize use of personal health information to train future AI algorithms as long as the potential for such use is “sufficiently describe[d] . . . such that it would be reasonable for the individual to expect that the protected health information could be used or disclosed for such future research.”[[47]](#endnote-47)

##### Interfacing with AI Vendors

Many pharmaceutical and medical device companies use AI vendors or services to complement (or in some cases completely outsource) their development and management of AI systems.

GDPR Compliance

Under the GDPR, these AI vendors constitute data processors. Companies should be mindful of the GDPR’s requirements for data controllers and processors and should ensure that their relationships with AI vendors comply with these requirements. To the extent possible, companies should consider using anonymized data for AI algorithms prior to transferring it to an AI vendor. Companies should also, to the extent possible use anonymized data even when the verdure does not have access to the data, for example in the case of using vendor cloud storage and processing services.

CCPA Compliance

Under the CCPA, disclosure of California consumers’ personal information to AI vendors may constitute a “sale” if the vendor is permitted to use the data for to train its algorithm for its own commercial benefit. As defined under the CCPA, “sales” include disclosures and transfers of personal information for “monetary or other valuable consideration.”[[48]](#endnote-48) Disclosure of non-anonymized personal information to a vendor as part of a service contract likely falls within that definition. To avoid this, companies should anonymize data for AI algorithms prior to transferring it to an AI vendor.

The CCPA does provide an exception for sharing personal information with a service provider to the extent such disclosure is “necessary to inform a business purpose.”[[49]](#endnote-49) However, that exception expressly requires that the service provider does not “further collect, sell, or use the personal information of the consumer.”[[50]](#endnote-50) Thus, to the extent companies share non-anonymized data with AI vendors and those vendors later sell algorithms trained on that data to third-parties, use the data internally to train other algorithms, or otherwise use the data in any way not necessary for the performance of the contract, such use likely constitutes a “sale.”

To avoid having to disclose such sales, obtain consent for them where the personal information belongs to a minor, and respond to consumers’ right to opt-out of sales at any time, companies should consider both 1) anonymizing personal information before disclosing it to AI vendors and 2) contracting to prohibit AI vendors from “selling” disclosed personal information within the definition of the CCPA.

HIPAA Compliance

Anonymizing data helps avoid HIPAA compliance issues as well. In the United States, HIPAA generally prohibits disclosure of protected health information unless such information has been de-identified or disclosure has been expressly authorized by the patient. HIPAA does include an exception for disclosure of protected health information that is “preparatory to research.” However, to do so, HIPAA would require companies to partially anonymize the protected health information to form a “limited data set” and then contract with AI vendors to ensure that the vendors use and disclose that data set only for a limited set of agreed-upon purposes.[[51]](#endnote-51) Use of disclosed protected health information by an AI vendor to train systems that it then sells or discloses to third-parties, therefore, may constitute a violation of HIPAA.[[52]](#endnote-52)

##### Data Retention

When companies train AI systems with non-anonymized data, those systems remain subject to the provisions of the GDPR, CCPA, and HIPAA.

GDPR Compliance

Under the GDPR, the systems are therefore subject to the rights of access, erasure, data portability, objection, and restriction from processing. If and when companies need to use non-anonymized data to train AI systems, they should consider what steps they would need to take when data subjects invoke these rights, including removing a data subject’s personal information from their AI algorithms.

In addition, companies should implement privacy by design principles throughout their use of AI systems.[[53]](#endnote-53) These procedures allow companies to manage their use of AI technologies and will help prevent issues with data security. Further, companies should consider whether and to what extent their use of AI requires them to perform Data Protection Impact Assessments (DPIAs) under GDPR Article 35. AI appears to warrant DPIAs, especially in the clinical context, as they are required “[w]here a type of processing in particular using new technologies . . . is likely to result in a high risk to the rights and freedoms of natural persons.”[[54]](#endnote-54) Article 35 permits, however, conducting one DPIA for an entire category of processing if the included processing activities are “similar” and present “similar high risks.”[[55]](#endnote-55)

CCPA Compliance

Under the CCPA, non-anonymized data that is retained by a company is subject to the consumers’ rights to notice, deletion, transparency concerning disclosure, opt-out of sale of personal information, and not to be subject to discrimination.[[56]](#endnote-56) If and when companies need to use non-anonymized data to train AI systems, they should consider what steps they would need to take when data subjects invoke these rights. Companies should also consider whether their use of personal information to train AI systems should be exempt from the right to deletion under the various exceptions in CCPA § 1798.105(d).

HIPAA Compliance

In the United States, non-anonymized data that is retained by a company or by an AI vendor remains subject to HIPAA’s requirements. Thus, AI algorithms trained using protected health information may not be disclosed nor used beyond the terms of patients’ informed consent without potentially violating HIPAA. Pharmaceutical and medical device companies, as well as their AI vendors, would also need to ensure that the AI systems comply with HIPAA’s security standards and would need to abide by HIPAA’s notification requirements in the event of breach.

# Appendix: GLobal & Regional Principles and frameworks

OECD Principles on Artificial Intelligence

In May 2019, the Organisation for Economic Co-operation and Development’s (OECD) released its “Principles on Artificial Intelligence.”[[57]](#endnote-57) The set of five principles for the ethical use of AI was compiled with input from the international, academic, and business communities.[[58]](#endnote-58) Though non-binding, the Principles are likely to be an influential benchmark for government and industry actors developing and using AI technologies. The OECD’s 36 member countries, as well as six additional countries – Argentina, Brazil, Colombia, Costa Rica, Peru, and Romania – have agreed to the principles. [[59]](#endnote-59) The European Commission has also given its support.

The OECD’s five principles for AI systems and the actors who use them are:[[60]](#endnote-60)

1. **Inclusive growth, sustainable development, and well-being -** Actors should use AI in a way that promotes growth for the benefit for all populations and reduces “economic, social, gender and other inequalities.”[[61]](#endnote-61)
2. **Human-centred values and fairness** - Actors should use proper “mechanisms and safeguards” to ensure that their use of AI complies with the “rule of law, human rights and democratic values,” including “freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognised labor rights.”[[62]](#endnote-62)
3. **Transparency and explainability -** Actors should “foster a general understanding of AI systems” and inform users that they are interacting with an AI system. Further, actors should enable users to understand the way the system works and the outcome it provides, such that users may easily challenge outcomes that adversely affect them.[[63]](#endnote-63)
4. **Robustness, security, and safety** - Actors should ensure that AI systems function properly and do not pose an “unreasonable safety risk” “in conditions of normal use, foreseeable use or misuse, or other adverse conditions.” This includes 1) ensuring that all “datasets, processes and decisions” are traceable throughout the AI lifecycle and 2) using a “systematic risk management approach” at each phase of the AI lifecycle regarding “privacy, digital security, safety and bias.”
5. **Accountability -** Actors should have responsibility for the “proper functioning of AI systems” and for their compliance with the above four principles.

Other multi-national working groups addressing the ethics of AI have made similar recommendations.

European Commission

The European Commission’s High-Level Working Group on Artificial Intelligence published a report entitled “Ethical Guidelines for Trustworthy AI” in April 2019. This report emphasizes the same values and principles as the OECD’s framework.[[64]](#endnote-64) These guidelines dictate that AI must be “lawful, ethical, and robust.”[[65]](#endnote-65) The guidelines do not discuss legal requirements other than to reinforce the “assumption that all legal rights and obligations that apply to the processes and activities involved in developing, deploying and using AI systems remain mandatory and must be duly observed.”[[66]](#endnote-66)

To be “ethical and robust,” AI must comply with four ethical principles: respect for human autonomy, prevention of harm, fairness, and explicability. To do so, actors should adhere to seven requirements:

1. human agency and oversight,
2. technical robustness and safety,
3. privacy and data governance,
4. transparency,
5. diversity, non-discrimination and fairness,
6. societal and environmental well-being, and
7. accountability.[[67]](#endnote-67)

In February 2020, the European Commission released a new white paper, “On Artificial Intelligence – A European approach to excellence and trust,” which reinforced the Commission’s support for a coordinated “ regulatory and investment oriented approach with the twin objective of promoting the uptake of AI and of addressing the risks associated with certain uses of this new technology.”[[68]](#endnote-68) This second paper sets forth a number of policy options to achieve these objectives and invites Member states, European institutions, and other stakeholders to respond. We understand that EFPIA and MedTech Europe are considering sharing feedback with the Commission. In particular, the report reemphasizes the importance of a regulatory framework that supports trustworthy and secure development of AI, and identifies elements of the EU legislative framework with potential relevance to AI applications. It also discusses possible adjustments to the existing regulatory framework, the scope of a future regulatory framework, types of requirements to be imposed, and compliance and enforcement. The white paper was accompanied by a companion resource, “The European Digital Strategy.”[[69]](#endnote-69)

International Panel on AI (IPAI)

France and Canada recently established the IPAI, which is a collaborative multi-stakeholder initiative with a mission “to support and guide the responsible adoption of AI that is human-centric and grounded in human rights, inclusion, diversity, innovation and economic growth.”[[70]](#endnote-70),[[71]](#endnote-71)

Though the panel is only just beginning to develop specific “best practices” for the use of AI, it published a declaration in May 2019 listing ten values for the use of AI. These include:

1. promoting a human-centric and ethical approach to AI,
2. supporting a multistakeholder approach to AI,
3. stimulating innovation, growth, and well-being,
4. adhering to principles of sustainable development,
5. strengthening diversity and inclusion,
6. fostering transparency and openness of AI systems,
7. fostering trust and accountability,
8. promoting democratic values, processes, and institutions,
9. bridging digital divides to provide access to AI across all populations, and
10. promoting international scientific collaboration.

United Nations Educational, Scientific and Cultural Organization (UNESCO)

UNESCO’s guidance is similar.[[72]](#endnote-72) It recently published preliminary guidance on the use of AI through the lens of its ROAM principles – “Rights, Openness, Accessibility, and Multi-stakeholder governance.”[[73]](#endnote-73) Specifically, the report suggests that AI should:

1. support freedom of expression, privacy, and equality,
2. promote transparency and openness to decrease “information inequalities,”
3. limit inequalities in access to AI technologies, research, data, and other resources, and
4. consider and incorporate perspectives of stakeholders influenced by the use of AI.[[74]](#endnote-74)

Council of Europe

Relatedly, the Council of Europe published its “Guidance on Artificial Intelligence and Data Protection” in early 2019.[[75]](#endnote-75) The document recommends that uses of AI:

1. respect human dignity and human rights, including the protection of personal data,
2. respect the principles of Convention 108+ (lawfulness, fairness, purpose specification, proportionality of data processing, accountability, transparency, data security and risk management),
3. avoid and mitigate risks,
4. respect the functioning of democracies and social and ethical values,
5. respect the rights of data subjects, and
6. allow meaningful control by data subjects over data processing.[[76]](#endnote-76)

canada’s office of the privacy commissioner

As of the time of writing, the Canadian government was in the midst of examining AI as it relates to the Personal Information Protection and Electronic Documents Act (PIPEDA). In early 2020, the Office of the Privacy Commissioner (OPC) released a request for comments on eleven proposals to ensure appropriate regulation of AI.[[77]](#endnote-77) Like many other regulatory bodies, this request acknowledged both the promise and challenges of AI, and described several possible approaches to reforming PIPEDA to strengthen privacy protection and achieve “responsible innovation.” Examples of some of the proposals presented include defining AI within the law to clarify which legal rules would apply to it; adopting a rights-based approach where data protection principles would be implemented as a means to protect a broader right to privacy; and creating a right to object to automated decision-making.

# REFERENCES

1. Nuffield Council on Bioethics, Bioethics Briefing Note: Artificial Intelligence (AI) in healthcare and research (2018), http://nuffieldbioethics.org/wp-content/uploads/Artificial-Intelligence-AI-in-healthcare-and-research.pdf. [↑](#endnote-ref-1)
2. Addressing the Data Challenges of Pharmacovigilence. Oracle. 2018. https://www.oracle.com/webfolder/s/delivery\_production/docs/FY16h1/doc34/Oracle-Pharmacovigilance-WP-R5.pdf?elqTrackId=a95a35aa97ad4956ae191686d4b25b8a&elqaid=67882&elqat=2 [↑](#endnote-ref-2)
3. Simon Smith, *141 Startups Using Artificial Intelligence in Drug Discovery*, BenchSci (Jul. 3, 2019), https://blog.benchsci.com/startups-using-artificial-intelligence-in-drug-discovery. [↑](#endnote-ref-3)
4. Med e-News, *AI key to finding MS biomarkers*, McGill Publications (2019), https://publications.mcgill.ca/medenews/2019/05/15/ai-key-to-finding-ms-biomarkers/. [↑](#endnote-ref-4)
5. *Id.* [↑](#endnote-ref-5)
6. World Economic Forum, *Global Agenda: Top 10 Emerging Technologies 2018* (Sep. 2018). [↑](#endnote-ref-6)
7. *AlphaFold: Using AI for scientific discovery*, DeepMind (Dec. 2, 2018), https://deepmind.com/blog/alphafold/. [↑](#endnote-ref-7)
8. *Id.* [↑](#endnote-ref-8)
9. *The Power of AI in Transforming Clinical Trials*, Biopharma Dive (Apr. 12, 2018), https://www.biopharmadive.com/spons/the-power-of-ai-in-transforming-clinical-trials/520795/. [↑](#endnote-ref-9)
10. Fuad Rahman, *The Past and Future of Clinical Trials – Part III*, Trials.AI (Jun. 17, 2019), https://labnotes.trials.ai/the-past-and-future-of-clinical-trials-part-iii. [↑](#endnote-ref-10)
11. *How it Works*, Deep 6 AI, https://deep6.ai/how-it-works/. [↑](#endnote-ref-11)
12. Casey Ross and Kate Sheridan, *Artificial Intelligence in drug discovery*, STAT, https://www.statnews.com/wp-content/uploads/2019/06/Artificial-intelligence-in-drug-discovery.pdf. [↑](#endnote-ref-12)
13. *Id.* [↑](#endnote-ref-13)
14. *Tempus Announces (TIME) Trial Service*, Tempus (Jun. 3, 2019), https://www.tempus.com/tempus-announces-time-trial-service-a-new-integrated-molecular-evaluation-that-leverages-artificial-intelligence-to-rapidly-match-cancer-patients-to-clinical-trials/. [↑](#endnote-ref-14)
15. *Id.* [↑](#endnote-ref-15)
16. Brite Health Co., https://britehealth.co/. [↑](#endnote-ref-16)
17. Seyedmostafa Sheikhalishahi, et al., *Natural Language Processing of Clinical Notes on Chronic Diseases: Systematic Review*, 7 JMIR Med Inform (2019); Feifan Liu, et al., *Natural Language Processing, Electronic Health Records, and Clinical Research*, *in* Clinical Research Informatics 296 (R.L. Richesson, et al., eds. 2012). [↑](#endnote-ref-17)
18. Antonio Regalado, *Google’s AI Explosion in One Chart*, MIT Technology Review (Mar. 25, 2017), https://www.technologyreview.com/s/603984/googles-ai-explosion-in-one-chart/. [↑](#endnote-ref-18)
19. Lily Peng, et al., *Deep Learning for Detection of Diabetic Eye Disease*, Google AI Blog (Nov. 29, 2016), https://ai.googleblog.com/2016/11/deep-learning-for-detection-of-diabetic.html. [↑](#endnote-ref-19)
20. University of California – Los Angeles Health Sciences, *AI performs as well as experienced radiologists in detecting prostate cancer*, American Association for the Advancement of Science (Apr. 16, 2019), https://www.eurekalert.org/pub\_releases/2019-04/uoc--apa041619.php. [↑](#endnote-ref-20)
21. Pesapane, 747. [↑](#endnote-ref-21)
22. Danton Char, et. al. *Implementing Machine Learning in Health Care – Addressing Ethical Challenges.* N Engl J Med

. 2018 March 15; 378(11): 981–983. [↑](#endnote-ref-22)
23. Pesapane, *supra* note 4, at 753. [↑](#endnote-ref-23)
24. Alim Bhatia, *The Dimensions of Ethical AI Changing the Face of Healthcare*, Towards Data Science (Apr. 27, 2019), https://towardsdatascience.com/the-dimensions-of-ethical-ai-changing-the-face-of-healthcare-3b72df1161e5. [↑](#endnote-ref-24)
25. *Ethics Guidelines for Trustworthy AI*, *supra* note 33, at 11. [↑](#endnote-ref-25)
26. *Ten Big Pharma Companies Collaborate on Data Sharing AI*, Drug Target Review (Jun. 7, 2019), https://www.drugtargetreview.com/news/44484/ten-big-pharma-companies-collaborate-on-data-sharing-ai/. [↑](#endnote-ref-26)
27. Council Regulation 2016/679 of Apr. 27, 2016, General Data Protection Regulation 2016 O.J. (L 119) 1, 3 art. 11 [hereinafter GDPR]; California Consumer Privacy Act, Cal. Civ. Code tit. 1.81.5, § 1798.145(a)(5) (2018) [hereinafter CCPA]; 45 U.S.C. § 164.514(a)-(b) [hereinafter HIPAA]. [↑](#endnote-ref-27)
28. GDPR art. 11; CCPA § 1798.110(d)(2); HIPAA § 164.514(2)(ii). [↑](#endnote-ref-28)
29. GDPR art. 4(1); CCPA § 1798.140(o)(1)(A). [↑](#endnote-ref-29)
30. GDPR art. 6. [↑](#endnote-ref-30)
31. GDPR art. 6(1)(a), (f). [↑](#endnote-ref-31)
32. GDPR art. 6(1)(a), (f). [↑](#endnote-ref-32)
33. *See* GDPR art. 9. [↑](#endnote-ref-33)
34. CCPA § 1798.140(g). [↑](#endnote-ref-34)
35. CCPA § 1798.100(b). [↑](#endnote-ref-35)
36. *Id.* [↑](#endnote-ref-36)
37. *Id.* [↑](#endnote-ref-37)
38. *See* CCPA §§ 1798.105, 1798.110, 1798.115, 1798.120, 1798.125. [↑](#endnote-ref-38)
39. *See* CCPA § 1798.150. [↑](#endnote-ref-39)
40. CCPA § 1798.150(a). [↑](#endnote-ref-40)
41. Department of Health and Human Services, Office for Civil Rights, Guidance on HIPAA and Individual Authorization of Use and Disclosures of Protected Health Information for Research (2018). [↑](#endnote-ref-41)
42. GDPR art. 6(1)(a), (b). [↑](#endnote-ref-42)
43. GDPR art. 22(1). [↑](#endnote-ref-43)
44. CCPA § 1798.100(b). [↑](#endnote-ref-44)
45. *Id.* [↑](#endnote-ref-45)
46. *Id.* [↑](#endnote-ref-46)
47. Department of Health and Human Services, *supra* note 68. [↑](#endnote-ref-47)
48. CCPA § 1798.140(t)(1). [↑](#endnote-ref-48)
49. CCPA § 1798.140(t)(2)(C). [↑](#endnote-ref-49)
50. CCPA § 1798.140(t)(2)(C)(ii). [↑](#endnote-ref-50)
51. CCPA § 164.514(e)(4)(ii). [↑](#endnote-ref-51)
52. CCPA § 164.514(e)(4)(iii). [↑](#endnote-ref-52)
53. See GDPR art. 25. [↑](#endnote-ref-53)
54. GDPR art. 35(1). [↑](#endnote-ref-54)
55. *Id.* [↑](#endnote-ref-55)
56. *See* CCPA§§ 1798.105, 1798.110, 1798.115, 1798.120, 1798.125. [↑](#endnote-ref-56)
57. *Forty-two countries adopt new OECD Principles on Artificial Intelligence*, OECD (May 22, 2019), https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm. [↑](#endnote-ref-57)
58. *Id.* [↑](#endnote-ref-58)
59. *Id.* [↑](#endnote-ref-59)
60. The OECD’s Principles also includes a list of recommendations for governments to implement “in their national policies and international co-operation, with special attention to small and medium-sized enterprises (SMEs).” These recommendations complement the report’s five principles and include: 1) investing in AI research and development, 2) fostering a digital ecosystem for AI, 3) shaping an enabling policy environment for AI, 4) building human capacity and preparing for labour market transformation, and supporting 5) international co-operation for trustworthy AI. *See* OECD, *supra* note 1. [↑](#endnote-ref-60)
61. *Id.* [↑](#endnote-ref-61)
62. *Id.* [↑](#endnote-ref-62)
63. *Id.* [↑](#endnote-ref-63)
64. Independent High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, at 2 (Apr. 8, 2019) [hereinafter *Ethics Guidelines for Trustworthy AI*]. [↑](#endnote-ref-64)
65. *Id.* [↑](#endnote-ref-65)
66. *Id.* at 2, 6. [↑](#endnote-ref-66)
67. *Id.* at 8. [↑](#endnote-ref-67)
68. *White paper on artificial intelligence,* European Commission (Feb. 2, 2020), <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>. [↑](#endnote-ref-68)
69. *European digital strategy,* European commission (Feb. 2, 2020), https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy. [↑](#endnote-ref-69)
70. *France and Canada create new expert International Panel on Artificial Intelligence*, Government of France (Dec. 7, 2018), https://www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence. [↑](#endnote-ref-70)
71. *Mandate for the International Panel on Artificial Intelligence*, Government of Canada (Dec. 6, 2018), https://pm.gc.ca/en/news/backgrounders/2018/12/06/mandate-international-panel-artificial-intelligence. [↑](#endnote-ref-71)
72. UNESCO, *Steering AI and Advanced ICTs for Knowledge Societies* (Mar. 5, 2019). [↑](#endnote-ref-72)
73. *Id.* [↑](#endnote-ref-73)
74. *Id.* [↑](#endnote-ref-74)
75. Eur. Consult. Comm. of the Convention for the Prot. of Individuals with Regard to Automatic Processing of Pers. Data, *Guidelines on Artificial Intelligence and Data Prot.*, Convention 108, Doc. No. T-PD(2019)01 (2019). [↑](#endnote-ref-75)
76. *Id.* [↑](#endnote-ref-76)
77. Consultation on the OPC’s Proposals for ensuring appropriate regulation of artificial intelligence: Seeking views on the OPC’s recommendations to Government/Parliament, Office of the Privacy Commissioner of Canada (Jan. 28, 2020), <https://priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-ai/pos_ai_202001/>. [↑](#endnote-ref-77)