Coping with the Mystery and Reality of Artificial Intelligence in Health Care[1]

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

[1] The author gratefully acknowledges the invaluable assistance provided in the preparation of this paper by Gregory E. Fosheim, an Associate in the McDermott Will & Emery Health Industry Advisory Practice based in the Firm's Chicago office, and Adriana Fortune, an Associate in the McDermott Will & Emery Health Industry Advisory Practice based in the Firm's Boston office,

I. INTRODUCTION

Artificial Intelligence in Health Care Overview

"Artificial intelligence (Al) systems and applications are ubiquitous in human life."[2] They recommend movies, **give** directions on the fastest routes to travel, detect credit card fraud, fulfill online purchases, drive cars and translate webpages into different languages.[3] While estimates of the impact of Artificial Intelligence ("**AI**") on the global economy are difficult to pin down, one recent report suggests a 14% effect on global GDP by 2030, half of which is expected to come from productivity improvements.[4]

While once viewed predominantly with substantial doubt and skepticism, and skeptics still abound,[5] use of Artificial Intelligence ("**AI**") technology has rapidly evolved and is now viewed widely with cautious optimism (rather than exuberance) as a real and viable, *albeit* quite virtual and mysterious, solution for improving health care diagnosis and treatment, technology vendors, entrepreneurs and investors. The following is but a small sample of the many recent and promising health care applications of AI:

- Reading medical images so as to improve accuracy of diagnoses and avoid missed diagnoses[6] in radiology, dermatology and anatomical pathology and other specialties that rely heavily on imaging technology, and to develop next generation radiology tools.[7]
- Managing what has become overwhelming demands on, and in some geographic areas of the U.S. and foreign countries the shortage or absence of, physicians,[8] particularly radiologists and anatomical pathologists,[9] and alleviate stress of burnout that are driving physicians out of practice.[10]

---

[2] Daniel, G. *et al.,* Duke Margolis Center for Health Policy, "Current State and Near-Term Priorities for AI-Enabled Diagnostic Support Software in Health Care," *available at* https://healthpolicy.duke.edu/sites/default/files/atoms/files/dukemargolisaienableddxss.pdf ("**Duke White Paper**"). *See also* Bresnick, J., "Arguing the Pros and Cons of Artificial Intelligence in Healthcare," HealthIT Analytics (September 2018), *available* at https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificial-intelligence-in-healthcare ("**HealthIT Analytics Pros & Cons**")

[3] *Id.*

[4] Challen et al, "Artificial intelligence, bias, and clinical safety," 8 BMJ Qual. Saf. 231 (2019) (**Challen"**).

[5] *See, e.g.,* Walker, J. , Loftus, P. and Abbott, B., "CEOs in Health Care Discuss Challenges of Working with Artificial Intelligence," *available at* https://www.wsj.com/articles/ceos-in-health-care-discuss-challenges-of-working-with-artificial-intelligence-11556724253; HealthIt Analytics Pros and Cons, *supra* at note 1.

[6] Grady, D., "AI Took a Test to Detect Lung Cancer. It Got an A," The New York Times (May 20, 2019), *available at* https://www.nytimes.com/2019/05/20/health/cancer-artificial-intelligence-ct-scans.html?mod=djemAIPro; Mukherjee, S., "AI v. M.D. – What happens when diagnosis is automated," The New Yorker (March 27, 2017) *available at* https://www.newyorker.com/magazine/2017/04/03/ai-versus-md

[7] *Id.;* Bresnick, J., "Top 12 Ways Artificial Intelligence Will Impact Healthcare," HealthIT Analytics (April 30, 2018), *available at* https://healthitanalytics.com/news/top-12-ways-artificial-intelligence-will-impact-healthcare ("**HealthIT Analytics Top 12**"); Krizhevsky, A., I. Sutskever, and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," ACM Digital Library. 2012: NIPS'12 Proceedings of the 25th International Conference on Neural Information Processing Systems, pp. 1097 – 1105.

[8] The U.S. has a dangerous physician shortage, particularly in rural regions and in developing countries. *See* https://healthitanalytics.com/news/arguing-the-pros-and-cons-of-artificial-intelligence-in-healthcare

[9] For examples regarding radiology, dermatology, and anatomical pathology, *see* Kent, J., "How Artificial Intelligence is Changing Radiology, Pathology" August 3, 2018), *available at* https://healthitanalytics.com/news/how-artificial-intelligence-is-changing-radiology-pathology; Mukherjee, S., "AI v. M.D. – What happens when diagnosis is automated," The New Yorker (March 27, 2017) *available at* https://www.newyorker.com/magazine/2017/04/03/ai-versus-md; , Health It Analytics Top 12 *supra* at note 6.

[10] https://patientengagementhit.com/news/how-does-provider-burnout-impact-patient-care-quality-care-access

- Combining the power of AI technology and big data with the exponential growth in next generation sequencing capabilities to accelerate the quest for development and deployment of precision-medicine solutions for diagnosing and treating cancer.[11]
- Reducing "diagnostic errors, which account for almost 60 percent of all medical errors and an estimated 40,000 to 80,000 deaths each year."[12]
- "[A]ugment[ing] clinicians' intelligence, support[ing] their decision-making processes, help[ing] them arrive at the correct diagnosis faster, reduc[ing] unnecessary testing and treatments otherwise resulting from misdiagnosis, and reduc[ing] pain and suffering by starting treatments earlier."[13]
- Analyzing medications, vital signs and other data points to predict acute respiratory failure and show promise for predictions of other life threatening and emergent episodes.[14]
- Identifying infection patterns and highlight at-risk but asymptomatic patients so as to contain risk of antibiotic resistance.[15]
- Using AI in an imaging system to give diagnostic information for skin cancer in patients.[16]
- Using AI algorithms in an electrocardiogram (ECG) device to estimate the probability of a heart attack using a smart that estimates the probability of a heart attack.[17]
- Empowering smartphones as diagnostic tools in dermatology, ophthalmology and developmental diseases.[18]
- Efficiently and meaningfully processing the increasingly vast volume of information about "wellness, disease, treatments and prevention," so as to reduce clinician burden and enhance diagnosis and treatment decisions.[19]
- Freeing up the time of professionals and administrative staff by automating routine tasks such as Electronic Health Record documentation, administrative reporting and triaging of CT scans.[20]

Other current and potential uses of AI technology include clinical trial matching, drug discovery, predictive modeling; advancing immunotherapy for cancer patients by assisting with finding targeted therapies for individuals' unique genetic makeup; data curation and de-identification to improve analytic

---

[11] *See, e.g.,* John Pletz, "Tempus Signs 'Groundbreaking' Deal with Cancer Doctors Group," Crain's Chicago Business (December 21, 2017), *available at* http://www.chicagobusiness.com/article/20171221/BLOGS11/171229974?template=printart

[12] National Academies of Sciences, Engineering, and Medicine. (2015). "Improving Diagnosis in Health Care." *The National Academies Press*, *available at* https:j/www.nap.edu/catalog/21794/improving-diagnosis-in-health

[13] Duke White Paper, *supra* note 1.

[14] McCormick, John, "Hospital System uses AI to predict deadly conditions," WSJ Pro, *available at* https://www.wsj.com/pro/artificial-intelligence

[15] HealthIt Analytics Top 12, *supra* at note 6.

[16] *See* FDA Artificial Intelligence and Machine Learning in Software as a medical device, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device#whatis

[17] *Id.*

[18] *Id.*

[19] Duke White Paper, *supra* at note 1. Medical data is expected to double every 73 days by 2020, and for every hour spent with a patient, physicians spend two hours on administrative tasks and updating electronic health records.[19] Some project the volume of health-related data will reach yottabyte (10^{24}) gigabytes, The Medical Futurist (2016), *available at* http://medicalfutureist.com/artificial-intelligence-will-redesign-healthcare/

[20] See, e.g. Emily Mullin, *Artificial intelligence pinpoints nine different abnormalities in head scans*, Nature Medicine (Dec. 19, 2018) *available at* https://www.nature.com/articles/d41591-018-00003-4

value of electronic health record data to develop models to predict risk of mortality, hospital readmission, prolonged hospital stay, and discharge diagnosis' and logistics.[21]

Several leading law schools are preparing for the future role of AI generally, including Columbia, Harvard, Stanford, University of Chicago, William and Mary, and Yale. The courses to date touch on algorithmic bias and civil rights, liability for autonomous vehicle accidents, and regulating AI-powered applications and platforms.[22]

AI and Other Technology Collaborations Generally

Collaborations have become a prominent and potentially powerful vehicle for developing and implementing Artificial Intelligence innovations because no one can bring all the ingredients, including technology/innovation prowess, massive and multi-dimensional data, and the clinical and research prowess needed to teach and support commercialization of AI. The collaborators span a broad spectrum of stakeholders including, among others, tech companies (both large and small), universities, academic medical centers and their affiliated universities, large institutional integrated delivery systems, leading cancer, pediatric and other specialty hospitals, research institutes, foundations dedicated to accelerating treatment innovations and cures in particular disease states, clinical and next generation molecular sequencing laboratories, insurers, pharmaceutical, device and biomedical companies, big data providers, and entrepreneurs, all of whom bring something valuable to the table and varying motivations for being involved in delivering AI solutions that can help predict, prevent or more effectively respond to disease. These new relationships are clearly bringing to bear the power of multiple competencies, resources and game-changing perspectives to drive innovation in health care delivery and research.

The collaborators' cultures, approaches, sophistication, resources, goals and objectives align in some important respects, but not in others. Understanding the differences and developing ways to reconcile and strike the right balance between and among them, properly characterizing the participants' respective roles, and identifying, allocating an managing the relative risks and rewards, will be key to a successful, sustainable and compliant collaboration. Some very perplexing but fundamental questions exist in the minds of many industry leaders. Will the new players and long-standing industry stalwarts really know what it will take to work together? Will they be able effectively to identify and align around a common ground that can drive the proposed innovation to the finish line in a mutually beneficial way despite differing culture, traditions and motivations? Such questions may go unanswered for some time. Among the many significant collateral effects of this acceleration of AI and other digital health solutions are heightened legal and regulatory risks and associated risk-management challenges and the blurring of traditional roles, responsibilities and accountability of the players in various contexts that calls for new approaches to contractual arrangements between and among them.

Investment in Commercialization - Trends

Many health industry stakeholders are also diversifying their approaches to investing in, the development and commercialization of, Artificial Intelligence and other health care technology discoveries. Many stakeholders who have engaged primarily in passive royalty-based out-licensing arrangements are seeking

---

[21] Duke White Paper *supra* at note 1; Woolf, M., "Paging Dr. Bot" – The Emergence of AI and Machine Learning in Healthcare," (American Bar Association (October 2017), *available at* https://www.americanbar.org/groups/health_law/publications/aba_health_esource/2016-2017/october2017/machinelearning/ ("**Woolf**").

[22] Council, J., "Top Law Schools Add AI Courses," The Wall Street Journal (April 22, 2019) *available at* (https://www.wsj.com/articles/top-law-schools-add-ai-courses-11555925401). The courses include: Columbia – "The Technology, Business, Law, and Policy of AI", Stanford – "Regulating AI", Harvard – "The Ethics and Governance of AI", Stanford – law/computer science class regarding how federal agencies use AI, Chicago – "Artificial Intelligence" seminar, William and Mary – "Artificial Intelligence, Emerging Technologies, and Their Effects on the Legal Landscape", and Yale – "Artificial Intelligence, Robotics, and Law" – now part of "Regulating Emerging Technologies."

a more active investment role in the commercialization of healthcare technology discoveries.[23] "They are investing more and more and at an earlier stage than ever before"[24] in AI and other technology discoveries generated internally by the institution and/or its clinicians, scientists and other inventors and by external entrepreneurs and other third parties.

Legal and Regulatory Framework

The existing legal and regulatory framework was not developed with the "black box" nature of AI in mind, and remains complex and difficult to apply in this brave new world. The legal framework is beginning to adapt, but that change lags significantly behind the pace and proliferation of AI technology innovation in health care. Again, however, given the pace of AI technology innovation and collaborations and their "game changing" potential, there is no time to wait for the legal and regulatory framework to catch up. Therefore now is the time to plan for and to build an infrastructure for identifying, managing and overseeing the complex legal and regulatory compliance risks and other enterprise risks to support AI innovations and associated collaborations and investments.

* * * * *

This paper will: (a) review current and emerging applications of AI in health care diagnosis and treatment and the emerging collaborations and investment activity coalescing around AI development and deployment; (b) explore the unique and complex legal, regulatory and other enterprise risks arising from the "black box" nature of this technology (e.g., maintaining and assessing quality and safety; managing malpractice exposure against potential changes in applicable standards of care; adapting approaches to informed consents and responding to potential changes in the patient-provider relationship; navigating the FDA medical device regulatory landscape; reimbursement compliance product liability risk management; maintaining data privacy, security and integrity; anticipating and minimizing risk of damage to reputation and patient/consumer trust); (c) explore evolving compliance program considerations and compliance risk allocation issues and strategies in contractual collaborations for development and deployment of AI; and (d) provide associated compliance and contracting planning strategies and tools for achieving a workable balance between potential risks and potential rewards.

[23] Those interested in playing a more active and profitable role in AI and other digital health commercialization ventures include academic medical centers, leading cancer, pediatric and other specialty hospitals, leading researchers, medical research foundations, and charitable foundations devoted to the acceleration of better treatments and cures for particular disease states.

[24] "Hospitals Discover Their Inner Venture Capitalist," Modern Healthcare (April 9, 2016) http://www.modernhealthcare.com/article/20160409/MAGAZINE/304099982, Wolinsky, Howard, "Hospital Systems Investing in Startups Whose Products They Use," Modern Healthcare (July 11, 2015).

II. ARTIFICIAL INTELLIGENCE IN HEALTH CARE

A. Artificial Intelligence Primer[25]

1. Historical Underpinnings

a. In 1950, Alan Turing predicted that machines would be capable of thinking like humans by the 21st century.[26] In his presentation to the London Mathematical Society in 1947, he described how intelligent machines will work:

> "It has been said that computing machines can only carry out the processes that they are instructed to do. This is certainly true in the sense that if they do something other than what they were instructed then they have just made some mistake. It is also true that the intention in constructing these machines in the first instance is to treat them as slaves, giving them only jobs which have been though out in detail, jobs such that the user of the machine fully understands what in principle is going on all the time. Up till the present machines have only been used in this way. But is it necessary that they should always be used in such a manner? Let us suppose we have set up a machine with certain initial instruction tables, so constructed that these tables might on occasion, if good reason arose, modify those tables. One can imagine that after the machine had been operating for some time, the instructions would have altered out of all recognition, but nevertheless still be such that one would have to admit the machine was still doing very worthwhile calculations. Possibly it might still be getting results of the type desired when the machine was first set up, but in a much more efficient manner. In such a case one would have to admit that the progress of the machine had not been foreseen when its original instructions were put in. It would be like a pupil who had learnt much from his master, but had added much more by his own work. When this happens I feel that one is obliged to regard the machine as showing intelligence."[27]

b. This prediction preceded the coining of the term "Artificial Intelligence" by John McCarthy[28] as the science and engineering of making intelligent machines.[29]

2. The AI Technology "Black Box" – Variations Along the Human Intelligence Spectrum

Artificial intelligence is defined in various ways, encompasses a "constellation of technologies" and spans a spectrum of capabilities. Where along the spectrum of capabilities a particular AI solution falls will have a bearing on the associated compliance and liability

---

[25] For a helpful definitions of key AI-related terms, *see* Duke White Paper, *supra* at note 1; Panch, T., Szolovits, P., Atun, R., "Artificial intelligence, machine learning and health systems," Journal of Global Health 8(2): 020303 (December 2018), published online October 21, 2018 *available at* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6199467/ ("**Panch**"); and Jiang, F., Jiang, Y., Zhi, H., *et al.*, "Artificial intelligence in healthcare: past, present and future," Stroke and Vascular Neurology, 2017:2:e000101, doi:10.1136/svn-2017-000101 (June 2017) *available at* https://svn.bmj.com/content/svnbmj/2/4/230.full.pdf

[26] Tan, C. (2012). "Artificial Intelligence: Will Computers Pass the Turing Test by 2029? *Does* it Matter?" *Harvard University, available at* http://sitn.hms.harvard.edu/flash/2012/ai/

[27] Turing, A.M. (February 20, 1947) "Lecture to the London Mathematical Society, *available at* *https://www.vordenker.de/downloads/turing-vorlesung.pdf* .*See also,* Press, G. (February 19, 2017). "Alan Turing Predicts Machine Learning and the Impact of Artificial Intelligence on Jobs," forbes.com, a*vailable at* *https://www.forbes.com/sites/gilpress/2017/02/19/alan-turing-predicts-machine-learning-and-the-impact-of-artificial-intelligence-on-jobs/#2b6b50bb1c2b*

[28] *Id.*

[29] *Id. See also* https://www.sciencedaily.com/terms/artificial_intelligence.htm

risks. The closer the capabilities are to the "Black Box" characterization discussed below, the greater will be the degree of risk.

a. In general, Artificial Intelligence refers to the ability of a machine to perform a task that is normally done by humans, including problem-solving and learning**.** It is a broad scientific discipline with its roots in philosophy, mathematics, and computer science that aims to understand and develop systems that display properties of intelligence.[30] It should be distinguished from "Augmented Intelligence" which is meant to enhance rather than replace the capabilities of human decision-making.[31]

b. Subcategories of AI include, "Narrow Artificial Intelligence" which "refers to AI designed to address a specific application area (e.g., strategic games, autonomous vehicles)";[32] and "General Artificial Intelligence" or "Strong AI" which refers to AI "[d]esigned to fully mimic human reasoning or intelligence in any context, and is capable of conscious, abstract thought"[33] and to "think exactly like humans do",[34] without being explicitly programmed.[35]

c. "Black Box" in the AI context "[r]efers to software that does not explain how the input data are analyzed in order to come to a recommendation. This can be because the algorithm model is too complex to be understood by humans . . . or because the functionality is considered proprietary.[36]

As discussed further below, Black Box AI is more likely to be as a regulated "medical device" as software that does not provide an opportunity for a health care professional to review the basis of the information or treatment recommendation it provides.

3. Subcategories of AI Technology and Associated Capabilities

a. "Machine Learning" is a sub-discipline of AI that can be used to design and train software algorithms to learn from and act on data. An algorithm is software that provides a well-defined procedure that allows a computer to solve a problem. Through machine learning, algorithms learn associations of predictive power from examples in structured data through the application of statistical models to data. Machine learning uses a broader set of statistical techniques than those typically used in medicine. In the healthcare context, machine learning techniques analyze data and attempt to cluster patients' traits or infer the probability of disease outcomes. (Clustering is grouping subjects with similar traits without relying on outcome data.)

---

[30] Panch, *supra* at note 24. Other definitions include: (a) "The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages." (English Oxford Living Dictionary); (b) "(1) A branch of computer science dealing with the simulation of intelligent behavior in computers; (2) the capability of a machine to imitate intelligent human behavior." (Merriam-Webster dictionary)' and (c) "The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings." (Encyclopedia Brittanica)

[31] Duke White Paper, *supra* at note 1.

[32] *Id.*

[33] *Id.*

[34] "Key Definitions of AI that Explain its Importance," Forbes Feb. 14, 2018.

[35] E. Topol. Deep Medicine Basic Books. (2019) p. 70.

[36] Duke White Paper, supra at note 1.

b. "Deep Learning" refers to a newer form of machine learning techniques referred to as "Neural Networks". Deep learning methods have been responsible for many of the recent foundational advances in machine learning[37] and are regularly used in imaging analysis.

(i) Neural networks consist of layers connected nodes communicating with each other to extrapolate outcomes with each node looking for its own component while communicating degrees of "truth" with its connections to paint an aggregated outcomes picture.

(ii) Deep learning methods allow a machine to be fed with large quantities of raw (uncurated) data and to discover the representations necessary for detection or classification based on models with fewer assumptions about the underlying data and therefore are able to handle more complex data and to conduct non-linear analysis.[38] These techniques rely on multiple layers of representation of the data with successive transformations that amplify aspects of the input that are important for discrimination and suppress irrelevant variations.

(iii) Deep learning may be "supervised" or "unsupervised" depending on whether the algorithm is "locked" so that its function does not change, or is "adaptive" (also referred to as "continuous learning") in that it continuously modifies itself "so its behavior can change over time based on new data"[39] and produce different output over time.[40]

(a) "Supervised Learning"[41], also referred to as "Rules-Based Artificial Intelligence"[42], is one of the most established types of machine learning that has been deployed for various non-healthcare applications and refers to use of a training set of data to train computer programs to learn associations between inputs and outputs in data (i.e., "if X, then Y" type rules) through analysis of outputs of interest defined by a supervisor (typically human). Once associations or rules have been learned based on existing data they can be used to predict future examples.[43]

(b) "Unsupervised Learning"[44], also referred to as "Continuous Learning"[45] refers to computer programs that learn association or patterns in data without use of defined associations/patterns of interest and is able to identify previously undiscovered predictors, as opposed to simply relying on known associations.

(c) "Reinforcement Learning" refers to computer programs that learn actions based on their ability to maximize a defined reward. This approach is influenced by behavioral psychology and has been applied with considerable success in gaming

[37] *Id.*
[38] Panch*, supra* at note 24.
[39] *Id.*
[40] Duke White Paper, *supra* at note1.
[41] Tang, A, *et al.*, "Canadian Association of Radiologists White Paper on Artificial Intelligence in Radiology," 69 CANADIAN ASSOC. RADIOLOGIST J., 120 (2018) ("**Tang**"); Panch, *supra* at note 24.
[42]
[43] Tang, *supra* at note 40; Duke White paper *supra* at note 1.
[44] Tang, *supra* at note 40.
[45] Duke White Paper *supra* at note 1.

where there is perfect information, many possible options, and no real world cost of failure.[46]

c. Natural language processing methods extract information from unstructured data (e.g., journal articles, EMRs) to build structured medical data to be used with machine learning and deep learning algorithms.

Unsupervised or Continuous Learning AI algorithms have both benefits and risks. The benefits include the ability to "more precisely calibrate suggestions to specific demographic or geographic areas over time …"[47] On the other hand, "as software changes, the rate and distribution of false-positives may also change, potentially in ways that no longer have an acceptable benefit-risk profile." [48]

B. Glossary of Additional Terms

Attachment A includes a Glossary of additional terms used in this paper.

C. Provider and Patient Receptiveness v. Reluctance and Skepticism

The absence of a receptive context for adoption of any new technology, including AI, can limit its application in the health care context.[49] "In the end, the need for human contact may emerge as the deciding factor in the battle between artificial clinicians and human caregivers."[50]

1. PWC – YouGov survey (November 2016)

This survey of 12,000 people across 12 countries (Europe, Africa, Middle East) explored: (i) appetite to engage with AI and robots for healthcare; (ii) circumstances under which there is greater or lesser willingness to engage; and (iii) the perceived advantages and disadvantages of using AI and robots in healthcare (https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/ai-robotics-new-health.pdf)

Findings:

a. People are increasingly willing to engage with AI and robots if it means better access to healthcare

b. Speed and accuracy of diagnosis and treatment is a critical factor for people's willingness

c. Trust in the technology is vital for wider use and adoption, and the "human touch" remains a key component of a person's healthcare experience

d. Developed economies were generally less willing to rely on AI

---

[46] Tang, *supra* at note 40.
[47] Duke White paper, *supra* at note 1.
[48] *Id*.
[49] Panch at note24; Woolf *supra* at note 20 *citing* Ziad Obermeyer, MD and Ezekiel J. Emanuel, MD, PhD, "Predicting the Future – Big Data, Machine Learning, and Clinical Medicine," N. Engl. J. Med. (Sep. 29, 2016), *available at* http://catalyst.nejm.org/big-data-machine-learning-clinical-medicine/
[50] Woolf *supra* at note 20.

e. Emerging economies were significantly more willing to engage with new technologies, perhaps due to access constraints and quality disparities between public and private care.

f. Men generally more willing to engage with AI than women, though some significant geographic variances

g. Very little differences between age groups

h. Consumers were most willing to receive four types of service: (i) monitor a heart condition, take note of symptoms, and advise on treatment; (ii) administer a test that checks heart rhythm and make recommendations based on results; (iii) provide customized advice for fitness and health based on personal preferences and health records; and (iv) take and test a blood sample and provide results (range 30% to 37%).

i. 73% were willing to undergo minor surgery (e.g. cataract or laser eye surgery) performed by a robot instead of a doctor.

j. Respondents from less developed countries were also willing to have major surgery conducted by robots (Nigeria – 69%; Turkey – 60%; South Africa – 51%)

k. Perceived disadvantages:

(i) lack of trust in robots with AI to make decisions on what to do if something unexpected is found (47%)

(ii) Robots with AI are impersonal and people need the "human touch" when it comes to healthcare (38%)

(iii) Only a physician or human healthcare professional can make the right decisions for health treatments to understand the underlying complexities involved and to use intuition (36%)

(iv) The technology is not sufficiently to predict benefits or dangers (30%)[51]

2. Physician Fears and Skepticism[52]

a. Fear of physician replacement and elimination of the human element.[53]

b. Alteration of the traditional doctor-patient relationship beyond recognition.

c. Inability to validate the reliability of the data and the rationale for the recommendation produced by the AI solution (and corresponding malpractice implications).

[51] *See also* 2018 consumer survey conducted by Accenture https://www.accenture.com/us-en/insight-new-2018-consumer-survey-digital-health?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosvitals&stream=top-stories

[52] HealthIT Analytics Pros and Cons, *supra* at note 1.

[53] For examples regarding radiology, dermatology, and anatomical pathology, *See* https://healthitanalytics.com/news/how-artificial-intelligence-is-changing-radiology-pathology; https://www.newyorker.com/magazine/2017/04/03/ai-versus-md

III. OVERVIEW: CURRENT STATE OF AI DEPLOYMENT IN HEALTHCARE AND WHAT IS ON THE HORIZON

A. Clinical Applications – Select Examples

Following are just some of the many other current and emerging applications of AI in the clinical care context.

1. Diabetic retinopathy (IDx-DR software) (FDA-submitted). Use of an AI solution to analyze images of the eye taken by a retinal camera without clinician interpretation to detect signs of diabetic retinopathy that clinicians often cannot do because of the lack of early symptoms before the vision deteriorates. Data submitted in support of FDA approval showed the ability to predict the presence of more than mild retinopathy with 87% accuracy and absence of more than a mild presence with 90 percent accuracy.[54]

2. Stroke (Viz.ai ContaCT – FDA cleared and MaxQ-AI platform); (AccipioIx – FDA submitted); (VizCTP – FDA cleared). Viz.ai ContactCT is an AI solution that uses a stand-alone CDS Software tool to analyze CT scan results to aid providers in identifying the most appropriate treatment plan for a patient. The Max-Q-AI platform, Accipiolx, is an AI-enabled software workflow tool that aids physicians with identifying acute intracranial hemorrhage and prioritizing the treatment of strokes or head trauma.55

3. Distal Radial Fractures (Imagen Osteo Detect). This AI solution uses detection and diagnostic software that uses AI to analyze two-dimensional x-ray images for signs of distal radius fracture so as to mark the location of the fracture and aid in earlier diagnosis and reduction of unnecessary treatment and follow-up imaging.56

4. Sepsis (under development by Duke and many other systems), offer the possibility of monitoring patients in "real-time", processing a vast amount of real-time and other clinical data to alerting clinicians that timely clinical evaluation and potential treatment is needed.

5. Primary Care Dx Support (Human Dx Project (currently in clinical trials) applies collective intelligence and machine learning to uses collective intelligence that combines and analyzes data from multiple physician opinions to produce additional information that physicians can use to increase diagnostic accuracy.

6. Bring intelligence to devices and machines such as notifying physicians when a wearable device identifies an anomaly.[57]

---

[54] Duke White Paper *supra* at note 1, *citing* FDA. (2018). "FDA permits marketing of artificial intelligence-based device to detect certain diabetes-related eye problems." https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm604357.htm

[55] Duke White Paper *supra* at note 1, *citing* Ochs, R. (2018). "Accipiolx." *FDA.* Retrieved from Ochs, R. (2018). "Accipiolx." *FDA.* Retrieved from https:flwww.accessdata.fda.gov/cdrh docs/pdf18/K182177 .pdfhttps:flwww.accessdata.fda.gov/cdrh docs/pdf18/K182177 .pdf

[56] Duke White Paper *supra* at note 1, *citing* FDA. (2018). "FDA permits marketing of artificial intelligence algorithm for aiding providers in detecting wrist fractures." *FDA News Release.* Retrieved from https:flwww.fda .gov/newsevents/newsroom/pressannouncements/ucm608833.htm

[57] Health IT Analytics Top 12, *supra* at note 6; Woolf *supra* at note 20.

7. Bring clinical decision-making to the bedside, including use of a text-based chat system to interact with the machine-learning system, to enable physicians to be proactive, predictive, and preemptive as well as deciding when to discontinue care.58

B. Collaborations Involving AI

1. Artificial Intelligence and Deep Learning to Support Clinical Care Diagnosis and Treatment

a. Partners HealthCare and GE Healthcare [59] have establisheD a ten -year collaboration to accelerate the development, adoption and integration of Artificial Intelligence and deep learning into every aspect of the patient journey from admittance to discharge. The collaboration is focused on co-development of open platform on which deep learning applications can be created, validated and seamlessly integrated into clinical workflows across the entire continuum of care and a broad spectrum of medical specialties, including radiology, pathology, genomics and population health, and ultimately shared with hospitals and clinics around the world so as to "… [bring] together hospitals, data sets and clinical and technical minds . . ."

Initial focus is development of applications to improve clinician productivity and patient outcomes in diagnostic imaging by "… empowering clinicians with the tool needed to store, analyze and leverage the flood of information to more effectively deliver care to patients."[60] For spinal injury, for example, clinicians currently deal with the fact that a lumbar spine MRI may generate up to 300 images and the need to review prior EMR scans and notes while at the same time facing critical decisions that have to be made almost immediately.

Future applications will be selected based on clinical need, technical capability, and market appetite and not just what data is available and include prognostic impact of stroke, identifying fractures in the emergency room, tracking how tumors grow or shrink after the administration of novel therapies, and indicating the likelihood of cancer on ultrasound.

b. Google partnered with Aravind Eye Hospital (Madurai, India) to launch an algorithm that used 128,000 ophthalmologist-evaluated images of eyeballs to train a deep neural network able to detect diabetic retinopathy with a 97.5% accuracy rate.[61]

c. Tempus and University of Michigan have collaborated on a project for pancreatic patients at U-M whereby Tempus will provide genomic and transcriptomic sequencing along with its bioinformatics and machine learning platform to analyze data sets and identify patterns and potentially actionable treatments.[62]

---

[58] *Id.*

[59] *See* Partners HealthCare Press Release, (May 17, 2017), *available at* http://www.partners.org/Newsroom/Press-Releases/Partners-GE-Healthcare-Collaboration.aspx

[60] *Id.*

[61] https://venturebeat.com/2019/02/25/google-works-with-aravind-eye-hospital-to-deploy-ai-that-can-detect-eye-disease/

[62] https://www.businesswire.com/news/home/20170130005100/en/Tempus-University-Michigan-Announce-Pancreatic-Cancer-Collaboration

d. Dermatology AI Algorithm – Stanford and Google[63]

Stanford researchers recently created an artificial intelligence algorithm that is capable of analyzing skin conditions to determine severity remotely through use of a photograph of abnormalities in a patient's skin condition (e.g., lesions, bumps, moles) and an analysis of the photo using deep learning programs against a pre-existing database containing 130,000 images of skin conditions and information concerning whether they indicated skin cancer (assisted by a Google-produced image classification program). The algorithm has potential for being developed into a mobile health app that can make initial screenings possible at home.

e. Medical University of South Carolina and Siemens entered a 10-year partnership to engage in numerous platforms, including AI for predicting treatment options based on how other patients fared.[64] Specifically, a "digital twin" technology will be deployed to optimize patient and family experiences and maximize efficiency.[65]

f. Google Deepmind and Moorfields Eye Hospital (UK) collaborated on a project in 2016 to determine whether AI could help clinicians improve the way eye conditions are treated and diagnosed.[66] Results show that the system can recommend the correct referral decision for 50+ eye diseases with 94% accuracy, matching world-leading eye experts.[67]

g. Researchers from Harvard-Beth Israel Deaconess and the MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) placed first in two separate categories at the annual meeting of the International Symposium of Biomedical Imaging for their AI, deep learning, machine-learning algorithm that teaches machines to interpret imagines of lymph nodes to decide whether they contained breast cancer. The automated method was 92% accurate; human pathologists are 96% accurate; and combining automated and human efforts together yielded 99.5% accuracy.[68]

2. <u>Use of AI to Fuel Precision Medicine</u>

Personalized or Precision Medicine refers to medical practices that use genetic tests and family history information to develop preventive, diagnostic, and therapeutic interventions that are tailored to individuals on the basis of their specific genetic code. Simply stated, the goal of precision health is "to anticipate and prevent disease in the healthy and precisely diagnose and treat disease in the ill."[69]

---

[63] *See* Sy Mukherjee, Stanford's Artificial Intelligence is Nearly as Good as Your Dermatologist, Fortune (Jan. 26, 2017), http://fortune.com/2017/01/26/stanford-ai-skin-cancer/

[64] https://www.postandcourier.com/health/musc-siemens-forge-unlikely-partnership-aiming-to-use-ai-in/article_3a5723be-a9f8-11e8-ba97-c71049cbfa93.html

[65] https://www.siemens-healthineers.com/press-room/press-releases/pr-20180827030shs.html

[66] De Fauw et al., *Clinically applicable deep learning for diagnosis and referral in retinal disease*, 24 NATURE MEDICINE 1342 (2018) (available at https://deepmind.com/documents/239/De%20Fauw%20et.%20al%20Nature%20Medicine%202018%20.pdf)

[67] https://www.moorfields.nhs.uk/news/breakthrough-ai-technology-improve-care-patients

[68] https://www.bidmc.org/about-bidmc/news/artificial-intelligence-achieves-near-human-performance-in-diagnosing-breast-cancer; see also https://www.hsph.harvard.edu/ecpe/why-health-care-cios-embrace-ai/

[69] Lloyd Minor, Stanford School of Medicine, "Stanford Medicine, Google team up to harness power of data science for health care,: Stanford Press Release (August 8, 2016), *available at* https://med.stanford.edu/news/all-news/2016/08/stanford-medicine-google-team-up-to-harness-power-of-data-science.html

a. Stanford and Google[70]

This collaboration combines Stanford clinical care and research excellence with Google's cloud technology, analysis and interpretation capabilities (advanced machine learning) technology infrastructure and super-computing power, bringing together 3 areas of science: data science, life science research and clinical care "'to derive useful insights from data and apply It directly to the care of a patient in near real time and also make progress on research.'"[71] Google Genomics, which uses the same technologies that support Google Search and Google Maps will be used to support the development of Stanford's Clinical Genomics Service focused on genome sequencing to expand genomics research, and use new methods of "real-time" data analysis to help diagnose disease.

According to press releases, as the new service begins, data gathered from hundreds and then possibly thousands of genome sequencing will go into the Google Cloud Platform on which aggregated and anonymous data of other Stanford patients (including other blood tests) could be stored and used by Stanford on the Cloud to analyze, in a fast and secure way, which gene variants might be responsible for a patient's health condition. A "data curation team" will work with physicians to narrow the possibilities (but it is unclear whether that team is provided by Stanford or Google).

The press release reports that Google will serve as a Business Associate in accordance with HIPAA. PHI will be encrypted, both in transit and on servers, and all servers will be in the U.S.

b. IBM Watson Genomics and University of North Carolina

Recently-published results of a study employing IBM Watson for genomics cognitive computing [72] showed that "'molecular tumor boards empowered by [the cognitive computing technology of IBM Watson for Genomics] can significantly improve patient care by providing a fast, cost-effective, and comprehensive approach for data analysis in the delivery of precision medicine …"[73] The study involved the use of IBM Watson Health for Genomics to analyze retrospective data on actionable genetic variations identified by a tumor board and compared the results of the analysis to those of a panel of cancer experts in 1,018 cancer cases. Results show that IBM was more efficient than the UNC cancer specialists in identifying potentially beneficial clinical trials or therapies based on the genetics of the patients' tumors.

c. CancerLinQ, and Tempus and Precision Health AI: Big Data and Next Generation Molecular Profiling to Support Oncology Trial Matching and Precision Medicine (December 2017) [74]

Ten Year collaboration of CancerLinQ, Tempus and its partner Precision Health AI in which Tempus will get access to the CancerLinQ data library (encompassing 600,000

[70] Lloyd Minor, Stanford School of Medicine, "Stanford Medicine, Google team up to harness power of data science for health care, Stanford Press Release (August 8, 2016), *available at* https://med.stanford.edu/news/all-news/2016/08/stanford-medicine-google-team-up-to-harness-power-of-data-science.html.
[71] *Id.*
[72] William Kim *et al.,* "Enhancing Next-Generation Sequencing-Guided Cancer Care Through Cognitive Computing," in The Oncologist
[73] *Id.*
[74] John Pletz, "Tempus Signs 'Groundbreaking' Deal with Cancer Doctors Group," Crain's Chicago Business (December 21, 2017), *available at* http://www.chicagobusiness.com/article/20171221/BLOGS11/171229974?template=printart

patients as of the end of 2017 and is growing regularly) and Tempus will provide CancerLinQ with a stream of revenue together with technical expertise and knowhow that will enhance CancerLinQ's ability to clean, curate and analyze its data library as well as develop tools and applications for its members. This collaboration is one of "about 50 other deals Tempus has with research hospitals," which Tempus' co-founder and CEO projects will enable Tempus to "touch 15 percent to 30 percent of cancer patients next year."[75]

CancerLinQ is an initiative of the American Society of Clinical Oncology (ASC)) and its Institute for Quality, which was developed to build on opportunities to drive rapid understanding and innovation by quickly assimilating new information and appropriately deploying new advances while also delivering efficient and high-quality care to a rapidly growing and aging patient population. CancerLinQ is data informatics system designed to collect and aggregate the complete EHRs of large numbers of patients with cancer (not just pre-specified fields from a defined cohort) and analyze aggregated data to provide a wide range of quality improvement, quality assurance, and care coordination services on behalf of participating providers, such as quality benchmarking, real-time clinical decision support, clinical trial indexing, and the generation of treatment plan summaries to share with patients. It will also standardize the aggregated clinical data, which is often unstructured, disorganized and in different formats, into analyzable aggregated data and uses its unique optical character recognition and natural language processing algorithms to isolate key factors in the patient's treatment history (e.g., who the patients are, what dugs they have taken, how they have responded to those drugs, and what genomic factors seem to be driving their disease) and then validates those findings with a team of qualified healthcare professionals who curate the data before deploying its insights to benefit providers and patients for a variety of purposes, such as assessment of treatment effectiveness and safety in real-world populations, rapid development of new and updated clinical guidelines, drug safety monitoring, and assessment of patient outcomes after new treatments.[76]

Tempus is a clinical laboratory that performs next generation molecular sequencing on tumors that provides a deeper and broader analysis of tumor mutations across a much broader panel of genes than the traditional panel in order to assess whether a particular drug will be effective for a particular patient. It "has built a series of data pipelines to collect, cleanse, and analyze data, at scale, utilizing the most sophisticated technologies, including cloud-based platform, cluster computing, next generation sequencing, natural language processing and AI-assisted image recognition," which" in turn are powering a variety of clinical and research application to drive clinical decision support and cutting edge academic research."[77] It applies its Big Data capabilities to aggregate and integrate genomic data from the aggregated molecular sequencing with clinical data and research data from a variety of sources into a large library of data that can be analyzed by health care providers and researchers to support clinical trial matching and precision medicine on a wide scale. More specifically, the "Tempus O" system is a big data platform that "collects, cleanses, analyzes and applies that data, at scale," and "can be used as a standalone product or in conjunction with the company's sequencing and analytic

[75] *Id.*
[76] *See* Schilsky, Michels, Kearbey, Yu and Hudis, *Building a Rapid Learning Health Care System for Oncology: The Regulatory Framework of CancerLinQ*, JOURNAL OF CLINICAL ONCOLOGY, J Clin Oncol 32:2373-2379 (August 2014).
[77] "Tempus and Sanford Health Collaborate on Personalized Medicine Initiative," November 2, 2017 *available at* https://globenewswire.com/news-release/2017/11/01/1172372/0/en/Tempus-and-Sanford-Health-Collaborate-on-Personalized-Medicine-Initiative.html

offerings."[78] Tempus' goal is to assemble the data that has been lacking but that is essential to develop a plan of attack for cancer treatment, including "building the world' largest library of molecular and clinical data and an operating system to make that data accessible and useful."[79] It also sells anonymized data to drug companies and other health industry stakeholders.[80]

Precision Health AI is a start up in artificial intelligence.

d. Cleveland Clinic and IBM have partnered for 5 years to use Watson to data mine and help physicians provide a personalized and more efficient treatment experience in part by analyzing thousands of medical papers using natural language processing to inform treatment plans, analyze EHR data, and account for both personalized clinical care and broader population-focused management.[81]

3. Chronic Care Management

IBM Watson and Medtronic created a joint platform, Sugar.IQ, to serve as a digital diabetes assistant using Watson's artificial intelligence capabilities to assist users in monitoring glucose levels in response to different foods, insulin dosage levels, and activities of daily life.[82] IBM reports the relationship to be a "strategic technology partner.[83]"

4. Health Record and Claims Data Enhancements

A Research collaboration between IBM Watson Health and Brigham and Women's Hospital and Vanderbilt University Medical Center was announced in February 2019.[84] The collaboration will include focus on the use of AI to improve the utility of health records and claims data along with physician and patient user experience and interactions with AI technology.

5. Clinical Trial Matching

a. Mayo Clinic and IBM Watson Health created *Watson for Clinical Trial Matching* to enroll patients in Mayo's breast cancer clinical trials.[85] In the first 11 months after implementation, Mayo experienced an 80% increase in enrollment in systemic therapy trials for breast cancer and an associated reduction in time to screen an individual patient for matches.[86]

---

[78] "Tempus Unveils Tempus O, a Platform to Structure and Annotate Clinical Data at Scale", December 7, 2017, *available at* https://globenewswire.com/news-release/2017/12/07/1247682/0/en/Tempus-Unveils-Tempus-O-a-Platform-to-Structure-and-Annotate-Clinical-Data-at-Scale.html

[79] Maria Castellucci, *Arming Oncologists and Researchers with More Genomic Data*, MODERN HEALTHCARE (January 23, 2017), p. 4.

[80] Pletz, *supra* at Note 56.

[81] https://newsroom.clevelandclinic.org/2016/12/22/cleveland-clinic-ibm-collaborate-establish-model-cognitive-population-health-management-data-driven-personalized-healthcare/

[82] https://www.mobihealthnews.com/content/medtronic-ibm-watson-launch-sugariq-diabetes-assistant

[83] https://newsroom.ibm.com/announcements?item=122916

[84] https://newsroom.ibm.com/2019-02-13-IBM-Watson-Health-Invests-in-Research-Collaborations-with-Leading-Medical-Centers-to-Advance-the-Application-of-AI-to-Health

[85] https://newsnetwork.mayoclinic.org/discussion/mayo-clinics-clinical-trial-matching-project-sees-higher-enrollment-in-breast-cancer-trials-through-use-of-artificial-intelligence/

[86] https://www-03.ibm.com/press/us/en/pressrelease/53783.wss

b. Health Quest Systems, Inc., a four-hospital system in New York and Connecticut entered into an agreement with IBM Watson Health in March 2019 to deploy IBM Watson for Clinical Trial Matching.[87]

c. Tempus and Sanford Health have collaborated to identify targeted therapies and clinical trials for breast cancer patients. The collaboration will utilize Tempus' infrastructure for analyzing data at scale and using cluster computing, next-generation sequencing, natural language processing, and AI-assisted image recognition to drive clinical decision support and academic research.[88]

6. Behavioral Health

a. Tiatros Inc. established a PTSD program supported by IBM Watson Personality Insights and Watson Tone Analyzer APIs to monitor veterans' evolution, openness, optimism, and joyfulness. Tiatros experienced a 73% completion rate for veterans participating in the program, whereas most programs have a 10% completion rate in the first year after diagnosis.[89]

b. MedyMatch Technology (Israel) announced a collaboration with IBM Watson Health to bring MedyMatch's AI-based clinical decision support application to imaging professionals in emergency departments to assist with identifying intracranial bleeding due to head trauma and stroke.[90]

7. Patient/Consumer Education and Engagement

Catalia Health is part of the American Heart Association's Health Technology and Innovations Innovators Network. To that end, Catalia created a personal health care companion product that provides patients with heart health topics through a guided conversational approach that includes answers to basic questions.[91, 92]

8. Surgery

Medtronic acquired Mazor Robotics in September 2018 for $1.7B.[93] Mazor and Medtronic had previously collaborated to produce the Mazor X Stealth Edition, which was recently cleared by FDA for spine surgery that uses software to plan the surgical procedure, a robotic arm to guide implants and instruments, and real-time imaging feedback to continuously verify the surgical plan.[94]

[87] https://www.clinicaltrialsarena.com/news/ibm-watson-for-clinical-trial-matching/
[88] https://hitconsultant.net/2017/11/01/tempus-sanford-health-precision-medicine/#.XMi096BKiUk
[89] https://www-03.ibm.com/press/us/en/pressrelease/52251.wss
[90] https://www-03.ibm.com/press/us/en/pressrelease/51835.wss
[91] https://www.prnewswire.com/news-releases/catalia-health-joins-american-heart-associations-center-for-health-technology--innovation-innovators-network-300720983.html
[92] http://www.cataliahealth.com/how-it-works/
[93] http://newsroom.medtronic.com/phoenix.zhtml?c=251324&p=irol-newsArticle&ID=2381128
[94] https://www.therobotreport.com/mazor-x-stealth-spinal-us/

9. Nursing

The Florida Association of ACOs entered into a strategic partnership with Care Angel to offer Care Angel's AI and Voice powered Virtual Nurse Assistant to ACO members.[95] Care Angel offers the ability to answer questions, monitor patients, and provide quick answers.[96] Virtual nursing assistants are estimated to save the health care industry $20B annually.[97]

IV. KEY LEGAL AND REGULATORY COMPLIANCE PLANNING CONSIDERATIONS

The legal and regulatory compliance requirements applicable to Artificial Intelligence innovation fall into many of the same substantive compliance risk categories that have long applied to traditional modes of health care delivery and payment and that have historically been covered by well-established health system compliance programs. For various reasons, however, managing these legal and regulatory requirements and the associated enterprise risks of non-compliance can be more challenging and complex in the Innovation context than in other compliance contexts:

- The nature of the technology solutions varies far more widely than in the traditional health care delivery and payment context, which produces a wide variation in the facts and circumstances to which the compliance program risk management measures need to be applied;

- Many of the applicable laws and regulations pre-date the development of today's AI technologies and were not written with them in mind;

- Nearly every state has its own statutes and regulations and both long-standing and emerging state laws are often ambiguous and non-harmonized; and

- New laws, regulations and policy positions are evolving steadily at the federal and state level but not keeping pace with the rate of change in the Innovation technology itself.

As illustrated in the chart set forth in Attachment B, dozens of federal and state regulatory agencies are intently focused on oversight and enforcement of the multi-dimensional regulatory compliance dimensions of Innovation initiatives:

The media and the class action bar are also keenly interested in covering and casting a bright and harsh spotlight on perceived misuses and failures of compliance oversight in the context of AI and other Innovation.

A. FDA Regulation of AI/ML Software as a Medical Device

The Food Drug and Cosmetic Act (**FD&C Act**), which establishes the basis for the Food and Drug Administration' (**FDA)** regulation of the sale of medical devices, defines a "Medical Device" as any "instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article" that is "**intended for use** in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease…" [Emphasis added.][98] "**Intended use**" means the **objective** intent of the persons legally responsible for labeling the device, which can be manifested by expressions or by the circumstances surrounding the distribution of the product (e.g., text of the label or instructions for use, press releases, statements by

[95] https://www.prnewswire.com/news-releases/flaacos-partners-with-care-angel-to-bring-ai-and-voice-virtual-nurse-assistant-angel-to-florida-acos-300573738.html
[96] https://www.careangel.com/ai-and-voice-powered-virtual-nurse-assistant
[97] https://www.forbes.com/sites/bernardmarr/2018/07/27/how-is-ai-used-in-healthcare-5-powerful-real-world-examples-that-show-the-latest-advances/
[98] 21 U.S.C. § 321(h).

manufacturer representatives (in person, media coverage, presentations, social media), brochures).

The FDA regulates medical devices using a risk-based classification regime[99] All devices are subject to registration, listing and adverse-event reporting requirements.

- Low-risk devices (Class I) are only subject to the forgoing requirements.[100]
- Moderate risk devices (Class II), can be cleared via a pre-market approval or by demonstrating equivalence to an already approved device through the 510(k) process.[101] Most devices are cleared by the 510(k) process.
- High risk devices must be approved through a full premarket approval pathway (PMA)[102] and typically involve clinical trials and the presentation of extensive evidence of safety and efficacy to the FDA

The Food and Drug Administration's (**FDA**) interest in whether digital health technology, including clinical decision software, mobile applications, medical device data systems, electronic health records, machine learning and other forms of Artificial Intelligence, and other Health IT is designed, manufactured, used and maintained in a manner that minimizes risk to patient health has been the subject of great discussion and controversy in recent years. The FDA's assertion of jurisdiction over Health IT has been evolving and in many respects has created "gray" zones of regulatory compliance. Digital health innovators, investors, collaborators, institutional customers and consumers must understand and monitor this developing area of regulatory compliance.

Whether software is and should be regulated as a medical device has been a particularly gray and unsettled area. Through the years, some software products have been deemed exempt from FDA authority by policy or regulation, while other software products have been classified under their own FDA regulations or considered "components" or "accessories" to other devices and regulated under the same classification as the underlying "parent" device.[103]

Thus, for years, the medical device and software communities have struggled to reconcile FDA's guidance documents and public statements with FDA's statutes and regulations when assessing whether FDA would regulate their software products as medical devices and, if so, which category of FDA medical device requirements would apply. While a comprehensive review of the evolution of the FDA's policy and enforcement position affecting the regulation of digital health generally is outside the scope of this paper, a summary of key recent developments affecting Artificial Intelligence technology and solutions follows.

1. 21st Century Cures Act

The 21st Century Cures Act (**Cures Act**), which was signed into law on December 13, 2016, helps to deliver some welcome transparency and relief on this uncertain regulatory front by specifically excluding certain categories of software from the statutory device definition and, thereby, FDA jurisdiction.

a. Exclusions of Certain Software from FDA Definition of Medical Device

[99] 12 CFR 860
[100] 21 CFR 860.3
[101] *Id.*
[102] 21 CFR 860.3(c)
[103] See, General Principles of Software Validation Guidance for Industry and FDA Staff, Food & Drug Administration, Jan. 11, 2002; Medical Device Accessories –Describing Accessories and Classification Pathways Guidance for Industry and Food and Drug Administration Staff, Food & Drug Administration, Dec. 20, 2017.

Notably, the Cures Act amended the FD&C Act's definition of "device" to exclude from the definition of "medical device" software and mobile medical apps that meet the following four criteria:

(i) The software is not intended to acquire, process or analyze a medical image or a signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system;

(ii) The software is not intended for the purpose of displaying, analyzing or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

(iii) The software is not intended for the purpose of supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and

(iv) The software is not intended for the purpose of enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the 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.[104]

Also excluded from the device definition is a software category commonly known as "clinical decision support software" ("CDSS").CDSS is defined as software intended for the purpose of:

(i) displaying, analyzing, or printing medical information about a patient or other medical information (such as peer-reviewed clinical studies and clinical practice guidelines);

(v) supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and

(vi) enabling such health care professional to independently review the basis for such recommendations that such software presents so that it is not the 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.[105]

Note, however, that Cures Act gives the Secretary of HHS the authority to override these exclusions if s/he finds that use of such software function presents significant likelihood and severity of patient harm if it does not perform as intended **or if the software is likely to supplant versus support the clinical judgement of the user based on the opportunity to review the basis of the decision and the intended user and use environment**. In such case, the Secretary would issue a final order identifying the software function at issue by publication of a notification in the Federal Register that includes the finding, the underlying rationale and identification of the evidence on which the finding was based. The Cures Act authorizes the Secretary to consider the following factors in making such a finding:

[104] FDCA § 520(o)(1)(E).
[105] *Id.*

(i) the likelihood and severity of patient harm if the software function were not to perform as intended,

(vii) the extent to which the software function is intended to support the clinical judgment of a health care professional,

(viii) whether there is a reasonable opportunity for a health care professional to review the basis of the information or treatment recommendation provided by the software function; and

(ix) the intended user and user environment, such as whether a health care professional will use a software function that is intended to acquire, process, or analyze a medical image or signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system, whether a health care professional will use the software function.106

These factors suggest that the FDA will exercise this authority to override the exclusion of software from the FDA definition of medical device for Artificial Intelligence and other software that is intended to serve as the sole basis for a diagnostic or treatment decision and/or is a "Black Box" that does not enable an independent review of the basis for the AI software's recommendations.[107]

2. FDA Response to the Cures Act: Draft Guidance

a. In 2017, the FDA issued draft guidance[108] with its then current thinking as to how to revise four previously issued digital health final guidance documents for consistency with the Cures Act.[109] The guidance document indicated the FDA's intent to exclude from the definition of medical device and to remove them from the list of software and apps the FDA previously listed as ones over which it intended to exercise enforcement discretion software that provides: (i) administrative support of a health care facility; (ii) maintains or encourages a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition); (iii) serves as electronic patient records; and (iv) transfers, stores, converts formats, or displays clinical laboratory test or other device data and results, findings by a health care professional with respect to such data and results, general information about such findings, and general background

---

[106] *Id*.

[107] "Clinical and Patient Decision Support Software – Draft Guidance for Industry and FDA Staff, (2017) *available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/clinical-and-patient-decision-support-software*. *See also,* Daniel, G. *et al.,* Duke Margolis Center for Health Policy, "Current State and Near-Term Priorities for AI-Enabled Diagnostic Support Software in Health Care," *available at* https://healthpolicy.duke.edu/sites/default/files/atoms/files/dukemargolisaienableddxss.pdf

[108] "Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act: Draft Guidance for Industry and Food and Drug Administration Staff" (2017), *Available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/changes-existing-medical-software-policies-resulting-section-3060-21st-century-cures-act

[109] The four previous FDA guidance documents corresponding to these four software functionalities are: "General Wellness: Policy for Low Risk Devices", *Available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm429674.pdf; "Mobile Medical Applications" (2105), *Available at Available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm263366.pdf; "Off-The-Shelf Software Use in Medical Devices" (1999), *Available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/shelf-software-use-medical-devices; and Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices" (2015), *Available at* https://www.fda.gov/regulatory-information/search-fda-guidance-documents/medical-device-data-systems-medical-image-storage-devices-and-medical-image-communications-devices

information about such laboratory test or other device (unless such function is intended to interpret or analyze clinical laboratory test or other device data, results, and findings).[110]

b. These new exclusions do not cover functions such as those that: (i) relate to the diagnosis, cure, mitigation, prevention or treatment of a disease or condition; (ii) relate to the reduction of the risk of or help living well with certain chronic diseases or conditions (but FDA will continue to include such functionality in its enforcement discretion position); (iii) are intended to acquire, process, or analyze a medical image or signal from an in vitro diagnostic device or a pattern or signal from a signal acquisition system; or (iv) are intended to generate alarms or alerts or prioritize multi-patient displays and that involve the analysis or interpretation of laboratory test or other device data and results.

3. FDA Response to the Cures Act: 2017 FDA Digital Action Plan

In the last decade, while the FDA worked to address reliability and safety compliance issues with the software embedded in medical devices, thousands of standalone health and medical applications appeared which seemed to fall under no existing regulations.

In July 2017, also in response to the 21st Century Cures Act, the FDA announced its Digital Health Innovation Action Plan (**Plan**)[111] and has been actively implementing it. In the Plan, the FDA acknowledges that the traditional regulatory approach toward moderate and higher risk medical devices is not well suited for the fast-paced, iterative design, development and type of validation used for digital health software products today, and announced its intent to explore an innovative approach to the regulation of digital health products that consists of three prongs: (i) implementation of the Digital Health Software Precertification (PreCert) Program, (ii) issuance of new guidance, and (iii) an internal expansion of FDA's digital health capabilities.

4. FDA Digital Health Software Precertification (PreCert) Program

The Software Precertification (Pre-Cert) Program under development by the FDA is intended to accelerate market entry of digital health devices by creating a process to establish confidence in a software developer's capabilities to create and maintain digital health devices that meet the agency's standards for safety and effectiveness.

a. Background: "Software as Medical Device" (SaMD) - Definition and Guidance

(i) The term Software as a Medical Device is defined by the International Medical Device Regulators Forum (IMDRF)[112] as "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[113]

(ii) The FDA has categorized software for purposes of medical device regulation as follows:

"Software, which on its own is a medical device – is one of three types of software related to medical devices. The other two types of software related to medical devices

[110] See FDCA § 520(o)(1)(D).

[111] *Available at* https://www.fda.gov/downloads/MedicalDevices/DigitalHealth/UCM568735.pdf

[112] The IMDRF is a voluntary group of medical device regulators from Australia, Brazil, Canada, China, Japan, Russia, Singapore, and the United States and European countries which provides harmonized principles for individual jurisdictions to adopt based on their own regulatory framework.

[113] *Id.*

include software that is integral to a medical device (Software in a medical device) and software used in the manufacture or maintenance of a medical device."[114]

(iii) Background: IMDRF SaMD Risk Framework

In 2013, IMDRF formed the Software as a Medical Device Working Group (Workgroup) to develop guidance supporting innovation and timely access to safe and effective Software as a Medical Device globally.

(a) The Workgroup, chaired [115]by the FDA, settled upon the crucial definitions for Software as a Medical Device, an outline for risk categorization for Software as a Medical Device, the Quality Management for Software as a Medical Device, and the clinical evaluation of Software as a Medical Device.

(b) The outline for risk categorization designates four separate categories for SaMD, each with its own characteristics and unique requirements for clinical evaluation from I, low impact, to IV high impact.

(c) As outlined in the chart below, IMDFR's risk framework assigns risk categories I – IV to SaMD based on a combination of the State of the Healthcare situation or condition and the Significance of Information provided by the SaMD to the healthcare decision and identification of the SaMD as treating or diagnosing, driving clinical management, or informing clinical management.

(1) Significance of Information – Devices that are used directly in the treatment or diagnosis of patient illnesses are expected to obtain higher standards of clinical evidence, including obtaining both scientific and analytical validity, as well as assessing clinical performance. Applications that drive, or merely inform clinical management are associated with less stringent validation requirements.[116]

(2) State of Health Care Condition – When a SaMD is used as an intervention for critical health care condition, it must be tested more rigorously than if its intended use is in detecting non-serious illnesses.[117]

[114] Software as a Medical Device, Food & Drug Administration, https://www.fda.gov/medical-devices/digital-health/software-medical-device-samd
[115] *Id.*
[116] "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations, IMDRF Software as a Medical Device (SaMD) Working Group, Sept. 18, 2014.
[117] *Id.*

State of Healthcare situation or condition	Significance of Information Provided by SaMD to healthcare decision		
	Treat or diagnose	Drive Clinical Management	Inform Clinical Management
Critical	IV	III	II
Serious	III	II	I
Non-Serious	II	I	I

b. FDA Software Pre-Certification Pilot Program

The Software Precertification Pilot Program, as outlined in the FDA's Digital Health Innovation Action Plan, will help inform the development of a future regulatory model that will provide more streamlined and efficient regulatory oversight of software-based medical devices developed by manufacturers who have demonstrated a robust culture of quality and organizational excellence, and who are committed to monitoring real-world performance of their products once they reach the U.S. market.

This proposed approach aims to look first at the software developer and/or digital health technology developer, rather than primarily at the product, which is what we currently do for traditional medical devices. Because software products can be adapted to respond to glitches, adverse events, and other safety concerns quickly, the FDA is working to establish a regulatory framework that is equally responsive when issues arise to help ensure consumers continue to have access to safe and effective products. In the Pre-Cert program, the FDA is proposing that software products from pre-certified companies would continue to meet the same safety and effectiveness standard that the agency expects for products that have followed the traditional path to market.

This pilot is an important first step to help us explore and evaluate the program model to inform how we establish the Pre-Cert Program. Pre-Cert 1.0, the first version of the program that will be available for pilot testing within the FDA's current authorities in 2019, is limited to Pre-Cert pilot participants' software as a medical device (SaMD). As the FDA leverages insights from testing of Pre-Cert 1.0, we envision offering the voluntary program to manufacturers of software in a medical device (SiMD), and other software that could be considered accessories to hardware medical devices. FDA will consider software that meets the definition of device in section 201(h) (as amended by section 520(o) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) in developing the program.[118]

(i) In September 2017, the FDA selected nine companies out of over 100 applicants to participate in the development of the Software Pre-Cert pilot program: Apple, Fitbit, Johnson & Johnson, Pear Therapeutic, Phosphorus, Roche, Samsung, Tidepool, and Verily.

[118] https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program#program

(ii) The FDA's Pre-Cert Test Plan for 2019 was released for the purpose of refining how the *De Novo* submission process would work for Pre-Cert.

The FDA will test the model in 2019 with certain SaMD *De Novo* Requests from Pre-Cert pilot participants and internally using selected previously-reviewed SaMD submissions. During this test phase, the FDA will assess whether the **Excellence Appraisal** and **Streamlined Review** components together produce an equivalent basis for determining reasonable assurance of safety and effectiveness for a software product prior to its introduction to the market, as compared to the traditional paradigm.[119]

The Excellence Appraisal process is identifying the objective criteria and methodology that the FDA will use to pre-certify a company and decide whether a company can keep its precertification status, based on five excellence principles: patient safety, product quality, clinical responsibility, cybersecurity responsibility, and proactive culture. The FDA is currently considering two levels of precertification based on how a company meets the excellence principles and whether it has demonstrated a track record in delivering safe and effective software products.[120]

(iii) The FDA is developing a risk-based framework so that a pre-certified company can determine the premarket review pathway for their products. Potentially pre-certified companies could market their lower-risk devices without FDA premarket review or only a streamlined premarket review based on the company's precertification level and International Medical Device Regulators Forum (IMDRF) risk categorization. The FDA is planning to leverage the IMDRF framework to help determine the risk categorization of a SaMD product, incorporating information about the medical purpose of the SaMD and the seriousness of the medical condition that the SaMD is intended to treat. It is also considering appropriate means to educate patients and providers about the premarket review and post-market monitoring obligations for each SaMD risk category.[121]

(iv) The FDA is also working to identify the type of information that a pre-certified company would include in its premarket submission for the FDA to review software products for safety and effectiveness before patients access them, this would be a streamlined review process. The FDA is identifying the type of information that a pre-certified company may have access to about how its software product is performing with patients to support the regulatory status of the product and new and evolving product functions.[122]

5. 21st Century Cures Act: Breakthrough Devices Program

The 21st Century Cures Act also called for FDA to develop its Breakthrough Devices Program, for which it released final guidance on December 18, 2018. The goal of the Breakthrough Devices Program is to provide patients and health care providers with timely access to these medical devices by increasing the speed of development, assessment, and review, while maintaining the statutory standards for premarket approval, 510(k) clearance, and *De Novo* marketing authorization.

---

[119] Digital Health Software Pre-Certification (Pre-Cert) Program, Food & Drug Administration, https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program

[120] *Id.*

[121] *Id.*

[122] *Id.*

a. Devices eligible for the Breakthrough Devices Program must meet the following requirements:

   (i) The device provides for more effective treatment or diagnosis of life-threatening or irreversibly debilitating human disease or conditions.

   (ii) The device also meets at least one of the following:

   (iii) Represents Breakthrough Technology;

   (iv) No Approved or Cleared Alternatives Exist;

   (v) Offers Significant Advantages over Existing Approved or Cleared Alternatives; or

   (vi) Device Availability is in the Best Interest of Patients.[123]

b. All submissions for devices designated as Breakthrough Devices will receive priority review. Priority review places a submission at the top of the appropriate review queue and the submission receives additional review resources, as needed. Although priority review for devices is intended to help accelerate patient access to certain devices that are key to public health, the FDA's past experience with the Priority Review Program indicates that review times may take longer for Breakthrough Devices than for other devices because of the novel scientific issues these devices may raise.

c. To support sponsors needing timely resolution of potentially novel issues, FDA offers "sprint" discussions with the goal of reaching mutual agreement on a specific topic within a set time period (e.g., 45 days). The number, format, and duration of interactions within a sprint discussion may vary based on project needs and should be defined a priori by the sponsor and FDA. The final guidance on sprint discussions includes a variety of features to reduce the time associated with the development, assessment, and review of eligible devices such as:

   (i) Offering "sprint discussions" where sponsors and FDA team members work to quickly align on focused issues such as testing protocols;

   (ii) Enabling more flexibility in clinical study design;

   (iii) Disclosing FDA advisory committee discussion topics to device manufacturers at least five days in advance of meetings;

   (iv) Allowing sponsors to recommend their own external experts;

   (v) Providing regular status updates to discuss the general progress of the project, next steps or plans for future discussions; and

   (vi) Allocating additional staff to respond to questions.[124]

[123] Breakthrough Devices Program Guidance for Industry and Food and Drug Administration Staff, Food & Drug Administration, Dec. 18, 2018, https://www.fda.gov/media/108135/download.
[124] *Id*.

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

On April 2, 2019, the FDA published an exploratory white paper proposing a framework for regulating artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD). The deadline for submitting comments is June 3, 2019.

a. The white paper leverages practices from the FDA's current premarket programs and relies on IMDRF's risk categorization principles, the FDA's benefit-risk framework, risk management principles described in the FDA's guidance on when to submit a 510(k) for device modifications[125] and the organization-based total product lifecycle approach (also envisioned in the FDA's Digital Health Software Precertification (Pre-Cert) Program.[126]

b. The white paper notes that a variable to consider that sets AI/ML software apart from other SaMD, is a spectrum of dynamism ranging from "locked" to continuous learning. A locked algorithm provides the same result each time for the same input. Locked algorithms represent the less complex side of AI/ML software.

   (i) The FDA has recently approved a few medical devices that use locked algorithms, such as a device used to detect diabetic retinopathy, and a device designed to alert providers of a potential stroke in patients.

   (ii) Continuously learning algorithms on the other hand, adapt and change their 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. The FDA has not yet approved a device that employs a continuous learning algorithm.[127]

c. While the FDA recognizes that some modifications may not require premarket review under the current FDA medical device classification system, FDA anticipates that many modifications to AI/ML software will involve "algorithm architecture modifications and re-training with new data sets," which would be subject to premarket review.

d. The FDA white paper proposes a Total Product Life Cycle (TPLC) approach to modifications to AI/ML-based SaMD, based on several regulatory concepts: the IMDRF risk categorization principles, FDA's risk-benefit framework, principles in FDA's Software Modifications guidance and the quality and organizational excellence-based approach FDA envisions for the Digital Health Software Precertification ("Pre-Cert") Program.[128]

---

[125] *Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/deciding-when-submit-510k-change-existing-device*

[126] Digital Health Software Pre-Certification (Pre-Cert) Program, Food & Drug Administration, https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program

[127] 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, US Food & Drug Administration, April 2, 2019, https://www.regulations.gov/document?D=FDA-2019-N-1185-0001.

[128] *Id*.

The FDA identifies four general principles that the agency believes appropriately balance benefits and risks, while providing access to safe and effective AI/ML-based SaMD:

(i) Establish clear expectations on quality systems and good machine learning practices (GMLP).

GMLP, reflects the FDA's expectations that medical device manufacturers have an established quality system that adapts to appropriate standards and regulation. Specific to AI/ML-based SaMD, the FDA suggests relying on the Software Pre-Cert principles of culture of quality and organizational excellence for developers, and on its SaMD Clinical Evaluation Guidance for demonstrating analytical and clinical validation. The FDA provides examples of GMLP considerations applicable to SaMD, including:

(a) Relevance of available data to the clinical problem and current clinical practice;

(b) Data acquired in a consistent, clinically relevant and generalizable manner that aligns with the SaMD's intended use and modification plans;

(c) Appropriate separation between training, tuning, and test datasets; and

(d) Appropriate level of transparency (clarity) of the output and the algorithm aimed at users.[129]

(ii) Conduct premarket review for SaMD that require premarket submission to determine reasonable assurance of safety and effectiveness and provide clear expectations for manufacturers of AI/ML-based SaMD to manage patient risks throughout the lifecycle.

The white paper proposes a basis for modifications to AI/ML-based SaMD that relies on a "predetermined change control plan," which would be submitted during the initial premarket review of the device. The predetermined change control plan would include the types of anticipated modifications, "SaMD Pre-Specifications" (SPS), and the associated methodology, "Algorithm Change Protocol" (ACP), that would be used to apply the changes in a measured way designed to minimize patient risk. The extent to which SPS and ACP pre-approval would be applicable to support upcoming changes depends on many factors, including the kind of changes (particularly as they relate to intended use) and their potential to bring risks to patients.[130]

(iii) Expect manufacturers to screen the AI/ML device and utilize a risk management methodology and other approaches outlined in FDA Guidance documents in development, validation, and execution of the algorithm changes, both SPS and ACP.

(a) If an AI/ML-based SaMD has an approved SPS and ACP, and changes are inside the bounds of both the SPS and ACP, manufacturers would note the change in the pertinent records and file for reference.

(b) If, the change is outside the granted SPS and ACP (but supports the same intended use), the FDA recommends using a "focused review" unto the SPS and ACP.

[129] *Id.*
[130] *Id*.

(c) If the changes would trigger a new intended use, the change would fall subject to premarket review.[131]

(iv) Enable greater transparency to users and FDA using post-market real-world performance reporting for maintaining continued assurance of safety and effectiveness.

FDA expects manufacturers to oblige to the principles of transparency and real-world performance monitoring, through a variety of potential mechanisms. Transparency could be shown by:

(a) updates to FDA and collaborators;

(b) certifying that labeling changes effectively define modifications;

(c) updating the specifications or compatibility of impacted supporting devices, components or accessories; and

(d) creating procedures to inform users of updates.[132]

7. Deciding When to Submit a 510(k) for a Software Change to an Existing Device (October 25, 2017) (501(k) Guidance)[133]

The 510(k) Guidance assists in determining when a software, including firmware, change to a device may require a manufacturer to submit a new 510(k) premarket notification. The purpose of the 510(k) Guidance is to increase the predictability, consistency, and transparency of the "when to submit" decision-making process by outlining the applicable regulatory framework and guiding principles.

B. Supporting AI and other Digital Health Product Claims – Consumer Fraud/Deceptive Practices

1. Regulators will hold AI developers, manufacturers and users accountable for substantiating product/solution claims with sufficient evidence. While there is not clear guidance concerning what regulatory, normative, or other industry standards apply in the context of AI and other novel technology, AI entrepreneurs, investors and enthusiastic users must remain mindful of the need to understand and meet regulatory standards and user expectations for the evidence that supports the claims they make in the advertising and marketing of their products.

2. FTC and FDA have a long-standing joint memorandum of understanding to coordinate efforts in protecting consumers against injury and deception. Specifically, FTC has responsibility regarding truth in advertising of food, drugs, devices, and cosmetics; FDA has responsibility in preventing misbranding and overseeing all labeling and the truth or falsity in prescription drug advertising. Given the ambiguity whether artificial intelligence is a medical device, it is not entirely clear whose responsibility it is to patrol false, misleading, or puffery claims about what AI can do.[134]

---

[131] *Id.*

[132] *Id.*

[133] *Available at* https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM514737.pdf

[134] Vanian, J., "Some Artificial Intelligence Should Be Regulated, Research Group Says," Fortune (December 6, 2018) *available at* http://fortune.com/2018/12/06/artificial-intelligence-regulation-government/

3. FTC enforcement will likely focus on protecting consumer welfare under the FTC's false advertising jurisdiction (which is discussed in further detail in the privacy discussion in Section IV).[135]

C. Malpractice Liability

1. Standard of Care

a. The U.S. medical malpractice regime holds physicians to accepted reasonableness standards of care and assigns liability when the care provided by physicians constitutes negligence or recklessness and exposes others to unreasonable risk of harm.[136] In general, courts apply either a national standard (typically for specialties) or a state-specific standard and evaluate whether a physician's actions are consistent with the degree of skill, care, and learning which is possessed and exercised by members of the medical profession in good standing.[137]

b. Courts generally have applied a standard of care for physicians that is neither static nor rigid. Courts will take into consideration the totality of the circumstances, including the physician's specialty, resources available to the physician, and the advances of the medical profession at the time of the physician's alleged negligent act.[138] Courts have recognized that medical standards of care typically evolve over time in response to empirical research, scientific progress, and the development of new technology.[139]

c. Very few cases directly apply the issue of malpractice risk associated with the use of AI systems specifically, and case law has not yet established distinct principles for evaluating the medical malpractice standard of care in the context of AI systems.

(i) Given the black box nature of AI systems and the unique ways they are developed to perform their functions, determining liability may become difficult and complex.

(ii) Different actors performing different functions (including the AI system, its trainers, and those tasked with its maintenance) may be implicated, and the role and function of the health care practitioner may begin to change given the nature of some of these AI systems.

(iii) The practitioner may take on responsibility for AI system training or testing, for example. Further, the practitioner may be working with data and diagnostic information from tools chosen by the patient and not the physician.

---

[135] Marketing Your Mobile App: Get it Right from the Start, *available at* https://www.ftc.gov/tipsadvice/business-center/guidance/marketing-your-mobile-app-get-it-right-start. *See also* Complaint for Permanent Injunction and Other Equitable Relief, FTC v. Breathometer, Inc., 17-cv-314 (N.D. Ca. Jan. 23, 2017); *see also "Breathometer" Marketers Settle FTC Charges of Misrepresenting Ability to Accurately Measure Users' Blood Alcohol Content*, FED. TRADE COMM'N (Jan. 23, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/breathometer-marketers-settle-ftc-charges-misrepresenting-ability (FTC complaint for injunction alleged that the app and device was falsely advertised and the company engaged in deceptive practices, as its claims were never substantiated and it misrepresented its accuracy while the app and device were sold. Under the terms of the FTC settlement, Breathometer, Inc. are prohibited from making accuracy claims concerning any breathalyzer product unless the claim is supported by "rigorous testing." The company is required to notify and pay full refunds to all customers who request one.)

[136] *RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM,* § 6 (Am. Law Inst. 2009).

[137] 1 STEVEN E. PEGALIS, AMERICAN LAW OF MEDICAL MALPRACTICE § 3.3 (3d Ed. 2016).

[138] See STEVEN E. PEGALIS, *supra* note 6, at § 3.3.

[139] *Id.*

(iv) Patients may be more empowered to take more control of their health care and utilize physicians in different ways.

2. How liability should be allocated in such a complex environment presents many difficult questions, such as the following, the answers to which are likely to evolve over time:

a. Courts defer to expert testimony, custom, and practice guidelines from medical societies to determine whether appropriate medical judgment was used.[140] Who will be the expert providing testimony when the use or non-use of AI is before the court? Will it be a physician, a computer programmer, a data analyst, an engineer, or perhaps a bit of each?

b. Courts have a long history of ignoring industry custom and imposing more stringent standards of care if an industry is slow to adopt certain technologies or injuries that could have avoided the adverse outcome.[141] Does a physician breach a duty by not using AI when it is available?

c. Who caused the adverse result? The physician overseeing the AI? The company who manufactured and marketed the machine? The engineer who built the algorithm? The health system that purchased the AI and encouraged physicians to implement its use? [142] Based on the principles of *respondeat superior*, health systems could be the causative agent for failing exercise due care in supervising or training AI users, or, conversely, in failing to provide physicians with adequate facilities and equipment.[143]

d. Is a *person* the right entity to be liable for the patient's injury, or should the artificially intelligent machine have personhood?[144]

e. Because tort law compensates for foreseeable harm, is a misdiagnosis foreseeable? Because machine learning is often designed to find connections where human diagnosis cannot, how are those connections foreseeable?

f. Did the patient assume the risk by consenting to AI's use?

3. Artificial intelligence is likely over time to shift the standard of care and, as it does, the economics of health care, malpractice liability, and insurance coverage for AI-supported health care may need to shift as well.[145]

---

[140] BARRY R. FURROW, HEALTH LAW: CASES, MATERIALS AND PROBLEMS, 7th Ed. (1987)

[141] *See, e.g.,* The T.J. Hooper, 60 F2d 737, 740 (2nd Cir. 1932) ("Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.")

[142] *See,* H. Sullivan and S. Schweikart, *Are Current Tort Liability Doctrines Adequate for Addressing Injury Caused by AI?"*, 21 AMA J. ETHICS E160, 161-62 (2019) *available at* https://journalofethics.ama-assn.org/sites/journalofethics.ama-assn.org/files/2019-01/hlaw1-1902_1.pdf.

[143] 27 Am. Jur. 2d Employment Relationship § 356; *see also* T. Meera, *et al.*, *Hospital's liability in malpractice suits,* 30 J. MED. SOC. 1, 1-2 (2016).

[144] *See*, Roman V. Yampolskiy, *Could an artificial intelligence be considered a person under the law?*, THE CONVERSATION (Oct. 5, 2018) *available at* https://theconversation,com/could-an-artifical-intelligence-be-considered-a-person-under-the-law-102865.

[145] David C. Vladeck, *Machines without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 124 fn 25, 150 (2012). In this article, Professor Vladeck hypothesizes establishing personhood for self-driving cars to allow victims to sue the vehicle and for state laws to require the car to obtain insurance (through a pool of funds provided by the manufacturer, supplier, and purchaser).

4. However, the value and effectiveness of a particular AI solution will need to be supported by substantial evidence as changes to standard of care normally require robust peer-reviewed research, testing and validation.[146]

D. Informed Consent

As AI systems become increasingly common in diagnosing and evaluating patient conditions and treatment recommendations, "informed consent" may become an important feature of the patient-physician relationship and have a bearing on malpractice liability and compliance with federal and state consumer protection laws.

1. Effective informed consent requires that a patient fully understand the health care treatment that he or she is agreeing to undergo. While the requirement of informed consent emanates from the goal of a patient consenting to whatever is done to his or her body, it can logically be expanded to circumstances in which a physician relies on advice from technology to make or support medical judgments, particularly when the technology remains new and, perhaps, unproven or trustworthy in the eyes of the general public.

2. Query:

    a. Just as a patient may refuse prescribed treatment, should the patient not also be able to refuse diagnosis by a machine?

    b. If a patient has a preference to not turn over significant conclusions to an AI machine, then what sort of informed consent may be appropriate?

    c. If an AI system can quantify its confidence, should the informed consent process be different?

    d. If a patient is able to avoid AI diagnosis, should this impact the applicable standard of care the potential liability of the physician?

3. Failure to obtain informed consent can give rise to civil liability if the patient demonstrates that: (i) the health care provider failed to present risks and benefits of a course of treatment along with available alternative options; (ii) with full information, the patient would have declined the chosen course of treatment or non-treatment; and (iii) the chosen course, even though performed appropriately and skillfully, caused the patients injuries in a substantial way.

4. Whether and how health care providers should inform patients about the use of artificial intelligence in diagnosing, theorizing treatment options, or performing procedures is an ethical matter that is beginning to elicit serious discussion. Query:

    a. Do physicians have the computer science wherewithal to explain the technical nature of AI support?

    b. When using black box neural networks, do physicians know how an AI algorithm determined its recommendation?

    c. Is a physician obligated to explain to a patient how a treatment decision was made?

5. Whether a patient would have made a different decision had the use of AI been disclosed is a matter for the fact finder, but a recent survey of the lay public conducted across twelve countries

[146] Duke White Paper *supra* at note 1, citing a 2017 JASON report on AI.

found varying degrees of willingness to have AI involved in their health care depending on geography, gender, and type of procedure.[147] It is foreseeable that patients with rare diseases will consent to such technical advances as being desirable before they are fully ready for implementation out of a fear that the patient has no other options.

6. The FTC guidance on consumer notice and consent practices should be taken into account in developing consent practices for AI that involves patient engagement through wearables and other mobile devices. See discussion below under Privacy.

E. Ethical Considerations – Risk of Bias in Data Driving AI

1. Commentators' Views of the "Dark Side" of A.I.-powered Systems

a. ". . . 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. As their builders are learning, the data used to train deep-learning systems isn't neutral. It can easily reflect the biases – conscious or unconscious – of the people who assemble it. And sometimes data can be slanted by history, encoding trends and patterns that reflect centuries-old discrimination. A sophisticated algorithm can scan a historical database and conclude that white men are the most likely to success as CEOs; it can't be programmed (yet) to recognize that, until very recently, people who weren't white men seldom got the chance to be CEOs. Blindness to bias is a fundamental flaw in this technology . . ."[148]

b. "The most powerful algorithms being used today 'haven't been optimized for any definition of fairness' . . . [t]hey have been optimized to do a task."[149]

c. The complexity of deep learning algorithms, particularly their potential "black box" nature, makes it more difficult for even the most sophisticated programmers to understand exactly how the A.I. system makes any given choice.[150]

2. Potential Sources and Causes of Bias

a. Unintended consequences from provider biases (sexism, racism, discriminatory diagnoses) based on the historical human biases in the data that is informing the system.[151]

b. Lack of context of certain cultural norms (e.g., prescribing habits in one country vs. another).[152] For example, the Netherlands adopts a "search and destroy" approach to Methicillin-resistant Staphylococcus aureus and other superbugs.[153] If an AI is trained to

---

147 PWC YouGov survey (November 2016) regarding (i) appetite to engage with AI and robots for healthcare; (ii) circumstances under which there is greater or lesser willingness to engage; and (iii) the perceived advantages and disadvantages of using AI and robots in healthcare (https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/ai-robotics-new-health.pdf)

[148] Vanian, J., "Unmasking A.I.'s Bias Problem," FORTUNE (June 25, 2018), *available at* http://fortune.com/longform/ai-bias-problem/

[149] *Id.*

[150] *Id.*

[151] *See*, e.g., Zou, J. and Schiebinger, L., "AI can be sexist and racist – it's time to make it fair," 559 NATURE 324 (2018).

[152] *See, e.g.,* https://phys.org/news/2018-07-culture-embedding-ai.html; https://ai.shorensteincenter.org/ideas/2019/1/14/creating-ai-systems-that-take-culture-into-account-aps9l; https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf).

[153] https://www.economist.com/europe/2019/01/26/why-dutch-hospitals-are-so-good-at-beating-superbugs

prescribe antibiotics, that may run counter to Dutch healthcare norms of quarantine and prudent use of antibiotics.

c. Providers have their own bias, with one-third of treatment errors arising from "anchoring bias" or providers' tendency to rely too heavily on a single piece of information.[154]

d. Attempts to use data from the Framingham Heart Study to predict the risk of cardiovascular events in nonwhite populations led to biased results, with both overestimations and underestimations of risk.[155]

e. If clinicians always withdraw care in patients with certain findings (e.g., extreme prematurity or a brain injury), machine-learning systems may conclude that such a finding is always fatal.[156]

f. Given the importance of quality indicators, there may be a temptation to teach a machine-learning system to guide users toward clinical actions that improve quality metrics without necessarily reflecting better care.[157]

g. Clinical decision support systems could be programmed to generate increased profits for their designers or purchasers (e.g., recommending drugs, tests, or devices in which they hold a stake or by altering referral patterns) without clinical users being aware.[158]

h. Bias can arise (i) in cases where the data sources themselves do not reflect true epidemiology within a given demographic, for example population data biased by the entrenched over diagnosis of schizophrenia in African Americans; or (ii) in cases where an algorithm is trained on a data set that does not contain enough members of a given demographic, such as an algorithm trained on data primarily from older, white, men, which may provide poor predictive value for young native-Alaskan women.[159]

i. The "All of Us" precision medicine research cohort is aiming to develop representative data sets that can be used for AI training and validation.[160]

3. One commentator's view is that, as machine-learning tools are relied on for diagnosis and advice for treatments, they will need to be bound by core ethical principles that have guided clinicians, such as beneficence and respect for patients.[161]

F. Products Liability

1. Developers, users, and manufacturers of AI tools must also understand and calculate product liability risks associated with the impacts of product failure or malfunction in a clinical setting. An AI tool that engages in clinical decision making in combination with or in lieu of a clinician may be considered a dangerous or high risk product under common law theories of liability and

---

[154] "The Robot Will See You Now" The Atlantic (2013).
[155] Gijsberts CM, "Race/ethnic differences in the associations of the Framingham risk factors with carotid IMT and cardiovascular events", PLOS/ONE (July 2, 2015) *available at* https://journals.plos.org/plosone/article?id=10.1371/journal.pone.013232
[156] Char, D.S. *et al.*, "Implementing Machine Learning in Health Care – Addressing Ethical Challenges", NEJM 2018 March 15,: 378(11) (**"Char"**).
[157] *Id.*
[158] *Id.*
[159] Vayena et al, "Machine learning in medicine: Addressing ethical challenges", 15 PLOS Medicine e1002689, November 2018.
[160] *Id.*
[161] Char *supra* at note 155.

various state consumer protection laws. The manufacturer, developer, or clinician could theoretically be held responsible for deficiencies or other problems associated with the use of the AI tool or the monitoring or interpretation of data produced by AI. In addition to the negligence regime discussed previously, product liability theories applicable to AI may also arise in strict liability and breach of warranty.

2. Manufacturers or developers may be held to a strict liability standard when a product is sold or used on a patient that contains an unreasonably dangerous defect in the design, manufacture or labeling of the product,[162] the defect causes harm to the consumer, and the harm results in actionable injury.

3. Manufacturers may similarly be held liable for a breach of warranty of merchantability when the manufacturer sells a product to a consumer that is not a reasonable fit for the purposes or intended use for which it was sold.

a. The elements for breach of warranty are similar to strict liability and can be asserted in jurisdictions that do not recognize strict products liability as a cause of action.

b. Does this standard have a role in evaluating and holding these types of AI systems accountable?

(i) The black box nature of AI systems may pose a challenge for the basic standard.

(ii) How can we tell if there is a defect?

(iii) Should the "trainers" of the AI system be evaluated; and if so, against what standard?

c. On the other hand, the social call for some strict liability standard may be heightened with direct-to-consumer AI products. If the products purport to provide actionable health related information or advice – particularly outside of a clinical setting – then, the risk of injury may increase.

4. Despite the existence of these and other product liability pathways, several courts have adopted the learned intermediary doctrine as a defense to the rule that manufacturers have a duty to warn patients about the risk of certain products.[163]

a. The doctrine protects manufacturers of prescription drugs and restricted (*e.g.* prescription) medical devices from product liability arising under failure to warn theories if the manufacturer provided adequate warning to the prescribing physician about the product's risks. If the defense is successful, the patient's remedy is limited to a medical malpractice or negligence claim against the physician.

b. The strength of the learned intermediary defense has eroded in recent years.

(i) Several courts have refused to apply the learned intermediary doctrine in personal injury actions involving prescription drugs and devices that were aggressively

[162] For example, a defibrillator with defective insulation that could trigger electric shocks in patients may constitute such a defect.

[163] RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB.§ 6 cmt. D (Am. Law Inst. 1998); *see also* J.S. Alain, *From Jeopardy to Jaundice: The Medical Liability Implications of Dr. Watson and Other Artificial Intelligence Systems*, 73 L.A. Law Rev. 1049, 1074 (2013).

marketed to the public through direct-to-consumer advertisements, Internet, and other forms of media.[164]

(ii) Courts have found that where the manufacturer's market efforts "drown-out" warnings and limitations on the use, the learned intermediary doctrine may not insulate manufacturers from liability.

5. With respect to AI systems within a clinical setting – and particularly those that are subject to training – some form of the learned intermediary doctrine may become more relevant. Whether this possibility disincentivizes manufacturers and developers from continuing to invest funds and talent on further improving AI's use in medicine remains to be seen.[165]

G. Data Quality

1. Over time, disease patterns change, leading to a mismatch between training and operational data.[166]

2. There is an ongoing need to:

a. Evaluate the adaptability of algorithms

b. Identify when software becomes stale or outdated

c. Work to anticipate expanded use and scalability of products

d. Ensure patient data is private and/or capable of being shared for research purposes while balancing innovation and privacy

3. Inaccurate or incomplete medical records can impair the quality of data used in AI solutions.

Query: If an AI system is able to digest copious information and learn from that information, is it biasing the results only to feed it the information that humans can extract? What if the information in an EMR is incorrect? Can AI "clean" that data? What if the data is accurate, but AI interprets it as an anomaly. Will that data be "cleaned" or will it be accepted and used for learning?

4. See Attachment C for "a general framework for considering artificial intelligence quality and safety issues in medicine."[167]

H. The Myriad of Federal and State Laws and Standards Applicable to the Collection, Sharing, Aggregation and Secondary Use Of Consumer Personal Health Information

1. Applicable Federal Laws include the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (and corresponding regulations); Children' Online Privacy Protection Act (COPPA)[168]; the Genetic Information Non-Discrimination Act (GINA); the Substance Abuse and Mental Health Services Administration regulations (confidentiality of data of individuals obtained

---

[164] *See, e.g., Centocor, Inc. v. Hamilton*, 372 S.W.3d 140 (Tex. 2012).

[165] *See*, J.S. Alain *supra* note 17 at 1074.

[166] Challen *supra* at note *3*

[167] Challen *supra* at note 3.

[168] 15 U.S.C. § 6501 *et seq.* (2003).

from a federally qualified substance abuse disorder programs (SAMSHA Rule));[169] the Federal Trade Commission Act (FTC Act); the Gramm-Leach-Bliley Act (GLBA)[170]; Fair Credit Reporting Act (FCRA)[171]; and the Telephone Consumer Protection Act (TCPA).

2. State laws include Constitutional Rights of Privacy, state statutes and regulations protecting confidentiality of general health information as well as sensitive categories of health information (e.g., HIV/AIDS, Mental/Behavioral health, Substance Abuse, Genetic Testing/Counseling), State Data Breach Notification Laws, State Data Disposal Laws, State Consumer Protection Laws, and State Common Law.

3. These laws vary from one another in various ways, including who is directly subject to the law (healthcare providers and plans, vendors, data processors, etc.); the nature and scope of the data covered (personal data, personal financial data, personal health data, personal data of children, general v. sensitive health data, other special categories such as racial origin, political/religious beliefs, sexual preference); the type of individual about whom the data is collected (adult, child), type of industry (e.g., health, banking/financial); and source/origin of the data regulated (e.g., direct from individual, medical records, health payment claims, indirectly through a health care provider or health place); and which government authority/official has jurisdiction to enforce the laws (HHS/OCR, FTC, FCC, State Attorney's General); and whether individuals have standing to enforce them.

I. FTC Data Privacy and Security Enforcement and Policy Initiatives

The FTC entered the data privacy and security enforcement fray with gusto, with a particular focus on the exposure of data companies collected from consumers. Health care related data collection and use practices are prominently featured in recent FTC oversight and enforcement, and it is collaborating with both ONC and the FDA in its effort to protect individuals who are both patients and consumers of digital health technology. While the FTC is unlikely to retreat from this active role, comments made by Acting Commissioner Maureen Ohlhausen early after being appointed to that position, indicate a focus on "actual harm," signaling a possible narrowing of the breadth of cases for which the FTC will initiate enforcement actions.

Acting Commissioner Ohlhausen also announced its plan to refine its legal framework for protecting the privacy and security of consumer information, which was launched with a workshop held by the FTC in December 2017 to explore how to characterize and measure the injury that a consumer suffers when information about them is misused. The workshop focused on three main components of the "informational injury" construct that has emerged from the FTC's recent case-by case privacy enforcement framework: (1) identify the different types of injury incurred by consumer and businesses from privacy and data security incidents; (2) determine an approach to quantitatively measure informational injuries and estimate the risk of their occurrence; and (3) better understand how consumers and businesses weigh these injuries and risks when evaluating the tradeoffs to sharing, collecting, storing, and using information. According to Acting Commissioner Ohlhausen, the FTC will use perspectives gained from the workshop in its development of a defined framework for enforcing informational injury within the agency's expansive Section 5 jurisdiction. Digital health innovators and other businesses whose strategies rely largely on the exchange of patient and other consumer personal information should watch closely as the FTC's privacy and security enforcement landscape continues to unfold.

1. Basis for FTC Jurisdiction over Data Practices – Section 5 of the FTC Act

[169] 42 C.F.R, Part 2.
[170] 15 U.S.C. § 94 (2012).
[171] 15 U.S.C. § 1681 (2003).

a. The FTC relies primarily on Section 5 of the FTC Act172 (FTC Act) as the jurisdictional base for its enforcement authority in this realm. Section 5 is a broadly written statute directed to "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." The only parameters the statute on its face imposes on the FTC's enforcement authority are that, for the FTC to intervene: (a) the act or practice must be likely to cause a substantial injury to consumers that is not otherwise reasonably avoidable, and (2) the negative impact of the act must not be outweighed by countervailing benefits to consumers or competition.173

b. Neither the FTC Act nor any corresponding regulation or subsequent act of Congress either expressly grants the FTC jurisdiction over data practices or declares data practices as an unfair or deceptive act or practice affecting commerce in which the FTC may intervene.

c. Whether the FTC Act nonetheless provides the FTC with a jurisdictional base to hold companies accountable for failing to safeguard consumer information was the very bone of contention in FTC v. *Wyndham*.[174]

2. FTC Health Data Breach Law for Non-Provider Health Industry Entities[175]

a. The FTC also has in its arsenal the data breach rules applicable to vendors of personal health records (**PHR**), PHR-related entities, and third-party service providers of vendors of PHRs and PHR-related entities. The FTC's rule requires entities to notify individuals promptly after gathering the necessary information concerning the breach and to notify the FTC within ten days of discovering the breach if the information involves more than 500 people; if the breach affects less than 500 people, the FTC requires notice within 60 calendar days following the end of the applicable calendar year. Finally, if the breach affects at least 500 residents of a given state, the entity must notify the media within 60 days after the breach and in any event without unreasonable delay. The breach notices provide a ready source of targets for investigations that could lead to further enforcement action by the FTC under Section 5 of the FTC Act.

b. Private Actions Triggered by Data Breaches

Data breaches have also triggered private lawsuits, increasingly ones brought as class actions, in both federal and state court. Following is a discussion of the salient litigation and compliance risk management insights emerging from some of the leading cases.

(i) Legal Theories Supporting the Claims

The menu of legal theories asserted by plaintiffs in these cases seems limitless, as they include among others: (c) violation of various federal statutes (e.g., FCRA,[176] the Privacy Act of 1974,[177] GLBA,[178] and COPPA,[179] Federal Declaratory Judgment Act[180]; (b) violations of

[172] 15 U.S.C. § 45(a) (2012).

[173] 15 U.S.C. § 45(n) (2012).

[174] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), 10 F. Supp. 3d 602, 613 (D.N.J. 2014).

[175] 16 CFR Part 318; *See* FED. TRADE COMM'N., *Complying with the FTC's Health Breach Notification Rule* (Apr. 2010), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf (last visited June 14, 2016).

[176] 15 U.S.C. § 1681 (2003).

[177] 5 U.S.C. § 552a.

[178] 15 U.S.C. § 94 (2012).

[179] 15 U.S.C. § 6501 *et seq.* (2003).

[180] 28 U.S.C. § 2201 (2006).

state statutes (e.g., data breach statutes, health and personal data protection statutes, patient rights statutes, medical professional and hospital licensure statutes) consumer protection statutes (fraud and deceptive practices and unfair trade or competition); and (c) state common law claims (e.g., negligence/gross negligence/negligence *per se*, invasion of privacy, identity theft, misappropriation of confidential financial information, breach of fiduciary duty, consumer fraud, negligent misrepresentation (e.g., by omission), breach of contract and implied contract, breach of covenant of good faith and fair dealing, detrimental reliance, and infliction of emotional distress).[181]

(ii) The Standing Hurdle

Regardless of the statute or common law theory underlying a data breach claim, plaintiffs are likely to face a motion to dismiss for lack of standing in both federal and state court. The standing challenges have been front and center in various prominent data breach cases decided by both federal and state courts since the U.S. Supreme Court's 2013 ruling in *Clapper v. Amnesty International USA*.[182] These cases provide valuable insights for crafting any data breach litigation strategy (on either side of the case) and for any privacy and security compliance program planning and risk management endeavor.

3. FTC IoT Guidance

The FTC is concerned about the privacy and security challenges faced by IoT. Its expressed concerns include the volume of data available for new analyses, potential for remote eavesdropping, potential for sharing of data consumers may not "reasonably" have expected, challenges and impracticability of providing notice and choice to consumers, and changes to the approach to providing notice and choice, increasing difficulty in defining and thus pinpointing health data subject to the mandatory notice and choice requirement, and security risks.

a. FTC Staff Report: The Internet of Things: Privacy and Security in a Connected World (January 2015) (the "**Internet of Things Report**")

The Internet of Things Report summarizes the proceedings and FTC Staff recommendations from the FTC's November 2013 workshop bearing the same name. The focus of the

---

[181] *See, e.g., In re Sony Gaming Networks and Customer Data Sec. Breach Litig.,* 996 F. Supp. 2d 942 (S.D. Cal. 2014), in which eleven plaintiffs from nine different states alleged 51 independent causes of action. Sony settled the case for $15 million in non-cash compensation (e.g., free games, game currency and subscription benefits), another $4 million for attorney fees, and notice of the settlement to potential class members. *See Peters v. St. Joseph Servcs. Corp.,* No. 4:14-cv-2872, 2015 U.S. Dist. LEXIS 16451; *In re Target Corp. Customer Security Data Breach Litig.,* 2014 U.S. Dist. LEXIS 175768 (D. Minn. Dec. 18, 2014) (finding that the plaintiffs had alleged sufficient harm in support of certain claims to deny the motion to dismiss). Target thereafter successfully settled the consumer case for $10 million, with final objections to the settlement being due on Nov. 10, 2015. *See* Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach gets Preliminary Approval*, N.Y. TIMES, Mar. 19, 2015, *available at* http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0. However, the settlement was subsequently overturned and remanded for further consideration on February 1, 2017. *See In re: Target Corp. Customer Data Security Breach Litig.*, No 15-3909, 2017 WL 429261 (8th Cir. Feb 1, 2017) (the 8th Circuit found the district court improperly certified the settlement class over the objection of a plaintiff). As of May, 2015, Target's settlement agreement with Mastercard for $19 million for a separate suit brought by financial institutions had fallen through. *See* Elizabeth Weise, *Target Breach Settlement with MasterCard Falls Through*, USA TODAY, (May 22, 2015), *available at* http://www.usatoday.com/story/tech/2015/05/22/target-breach-mastercard-visa/27782665 (last visited June 14, 2016). *See* Dittman v. Univ. Pitt. Med. Ctr., 2017 PA Super. 8 (Pa. Super. Ct. 2017) (holding an employer does not owe a legal duty to an employee to protect electronically stored personal and financial information against the risk of the criminal acts of superseding third-parties).

[182] 133 S.Ct. 1138 (U.S. 2013). The case dealt with the Foreign Intelligence Surveillance Act Amendments of 2008 that created a new framework under which the federal government could seek the Foreign Intelligence Surveillance Court's authorization of surveillance targeting communications of non-U.S. citizens abroad.

workshop was the consumer protection implications of the Internet of Thing devices sold to or used by consumers (as opposed to those sold or used in the business-to-business or machine-to-machine context.[183]

b. Best Practices

The Report identifies six "Best Practices" that companies should consider:

(i) Security by Design (e.g., "building security into … devices at the outset, rather than as an afterthought");

(ii) Personnel Policies (e.g., providing appropriate security training for relevant personnel and ensuring "that product security is addressed at the appropriate level of responsibility within the organization;

(iii) Service Providers (e.g., only engaging service providers who "are capable of maintaining appropriate security" and exercising reasonable oversight to ensure that service providers are actually providing appropriate security);

(iv) Defense-in-Depth (e.g., employing "multiple layers of security" to defend against threats, for example, encrypting certain data in transit and at rest instead of simply relying on a consumer's Wi-Fi router);

(v) Access Controls (e.g., "implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network"); and

(vi) Monitoring (e.g., providing support and security patches and weighing carefully decisions to cease such support that may make the devices vulnerable to security patches and being forthright with consumers on whether they will continue to provide such support).

c. The Report includes more specific discussion and recommendations for industry on three key topics: security, data minimization, and consumer notice and choice.

(i) Security

The report endorses "reasonable" security procedures, which it acknowledges will vary depending on a variety of factors, including "the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities." The FTC also released a separate security guide for businesses, entitled: "*Careful Connections: Building Security in the Internet of Things.*[184]

(ii) Data Minimization

The report identifies data minimization as a privacy risk mitigation strategy, noting that "collecting and retaining large amounts of data increases the potential harms associated with a data breach," and increases the "risk that the data will be used in a way that departs from consumers' reasonable expectations." At the same time, the FTC identifies the need to balance minimization of privacy risk with preserving the "flexibility to

[183] FED. TRADE COMM'N. (Staff Report), *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (last visited June 14, 2016).
[184] *Available at* https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things (*last visited June 12, 2016*).

innovate." Therefore, the report identifies various options for consideration in attempting to achieve this balance: "decide not to collect data at all, collect only the fields of data necessary to the product or service being offered, collect data that is less sensitive, de-identify the data they collect," and/or obtain consumer consent to collection.

(iii) Consumer Notice and Choice

The FTC staff believes that, although challenging to implement because of the ambiguity of data collection, practical obstacles to providing information without a direct user interface and the fact that there is no one-size-fits-all approach, consumer choice plays an important role in the IoT. Providing choice before collecting and using consumer data need not be mandatory when the practices are consistent with the context of a transaction or the company's relationship with the consumer because the uses are generally consistent with consumers' reasonable expectations and the cost of providing choice outweighs the benefits in the context of IoT generally. The benefit outweighs the burden (even potential limitations on beneficial new uses), however, when the use is inconsistent with consumers' reasonable expectations and the approach to providing choice should be clear and prominent, and not buried within lengthy documents. Options identified by the report include video tutorials, affixing QR codes on devices, and providing choices at the point of sale within set-up wizards or in a privacy dashboard. Particularly with regard to beneficial new uses of data, the FTC suggests that the company need not provide choice if it "de-identifies" the data "immediately and effectively". Finally, it suggests there is a need for legislation to address such secondary, potential risk of drawing inferences from the combination of collected data with other available data, and standards and approaches for addressing and achieving the appropriate balance between potential harms and benefits.

J. Creation and Use of Data Repositories

HIPAA treats the creation of a data repository using/containing PHI and the subsequent use of the repository as two separate events for which a compliance pathway must be established. The purpose for which the repository is being created will be a key factor in determining what compliance pathways are available for creating it.

1. Creation and use of a Repository Solely for Health Care Operations Purposes

a. HIPAA treats the creation of a data repository by a Covered Entity using only its PHI to be a health care operations function that can be undertaken without an authorization, waiver of authorization or HIPAA exception so long as the Covered Entity uses the repository only for other health care operations purposes.[185] A Covered Entity may also retain a business associate to create and/or host the repository for healthcare operations purposes pursuant to a valid Business Associate Agreement, without an authorization, waiver of authorization, or HIPAA exception.[186]

b. A Covered Entity may also create a shared repository with other Covered Entities and may retain a third party to assist with that undertaking pursuant to a valid Business Associate Agreement.[187] The nature and extent to which the PHI of one Covered Entity in the repository may be disclosed to and used by the other participating Covered Entities without

[185] 45 CFR § 164.501 (defining "health care operations").

[186] 45 CFR § 160.103 (defining "business associate"); 45 CFR § 164.502(e). A covered entity may also be the business associate of another covered entity.

[187] 45 CFR § 160.103 (defining "business associate"); 45 CFR § 164.501 (defining "data aggregation"); 45 CFR § 164.504(e)(2)(i)(B) (business associate agreement standards).

an authorization, waiver of authorization or HIPAA exception will vary. The broadest possible use will be by participants in an Organized Health Care Arrangement (**OHCA**) for the health care operations purposes of the OHCA.[188] If the participants are not in an OHCA, they may share only the information of individuals with whom they have both had a relationship and only for the health care operations activities listed in the first two paragraphs of the Privacy Rule's definition of "health care operations"[189] and fraud and abuse compliance activities.

2. Creation and Use of a Repository for "Research" purposes (within the meaning of HIPAA)[190]

a. The creation of a data repository itself is "research" within the meaning of HIPAA if the intent is to use it for research.[191] Therefore, under HIPAA, the creation of the repository will require an authorization or a waiver of authorization, unless the repository will contain only "de-identified" data or data comprising a "limited data set."

(i) However, a Covered Entity does not need either an authorization or a waiver thereof to disclose PHI to a business associate pursuant to a valid BAA to perform the expressly defined health care operations activity of creating de-identified data or limited data sets.[192]

(ii) Further, an authorization (or waiver thereof) is not necessary for a Covered Entity to disclose limited data sets for purposes of research pursuant to a valid Data Use Agreement.[193]

(iii) The business associate engaged to undertake the de-identification or create the limited data sets may also be a researcher who will receive the de-identified data or limited data set for use in conducting research, provided the Business Associate Agreement requires the recipient to return or destroy the identifiers once the limited data set has been created[194] (or provided there are robust firewalls, data governance protocols, and

---

[188] 45 CFR § 164.506(c).

[189] 45 CFR § 164.501(definition of "health care operations", subsections (1) and (2), which, in general terms, encompass a broad range of care management and quality improvement activities, as well as credentialing and training of professionals).

[190] Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. 45 CFR § 164.501 (defining "research").

[191] *See* NAT'L INST. OF HEALTH, *Research Repositories, Databases, and the HIPAA Privacy Rule*, NIH Publication Number 04-5489, p. 9 (Jan. 2004), *available at* http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf (last visited June 14, 2016) (in particular, the response to the question: "How may a covered entity use or disclose PHI for the creation of a research repository or database when it is unknown at the time of collection what specific protocols will make use of the repository or database in the future?").

[192] 45 CFR § 164.501 (defining "health care operation" as including "creating de-identified health information or a limited data set"); NAT'L INST. OF HEALTH, *Research Repositories, Databases, and the HIPAA Privacy Rule*, NIH Publication Number 04-5489, p. 9 (Jan. 2004), *available at* http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf (last visited June 14, 2016) (stating that a covered entity may hire a business associate to create a limited data set without patient authorization or a waiver thereof, provided it is "conducted in accordance with the business associate requirements at sections 164.502(e) and 164.504(e)").

[193] 45 CFR § 164.514(e)(3) (permitting a covered entity to "use or disclose a limited data set . . . for the purposes of research" pursuant to a data use agreement, and to "disclose protected health information only to a business associate for [the] purpose" of creating a limited data set).

[194] U.S. DEP'T OF HEALTH & HUMAN SERVS., *Health Information Privacy Frequently Asked Questions* (Mar. 14, 2006), *available at* http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/250.html; NAT'L INST. OF HEALTH, *Research Repositories, Databases, and the HIPAA Privacy Rule*, NIH Publication Number 04-5489, p. 9 (Jan. 2004), *available at* http://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf.

other necessary safeguards in place to segregate the research and business associate divisions of the entity).[195]

b. The subsequent use will also require a HIPAA compliance pathway (i.e., an authorization or a waiver of authorization, use of only "de-identified" data or use of data comprising a "limited data set" pursuant to a HIPAA-compliant Data Use Agreement).

3. The federal Common Rule governing research on human subjects (**Common Rule**)[196] and the Food and Drug Administration (**FDA**) laws governing the protection of human subjects in FDA-regulated research (the **FDA Law**)[197] also include privacy protections that coincide with HIPAA's in some respects but differ from HIPAA's in others. The consent requirements of the Common Rule and FDA Law must also be carefully analyzed in connection with the creation and use of a repository.

a. Research governed by the Common Rule is research that involves a human subject. The Common Rule defines a human subject as "…a living individual about whom an investigator (whether professional or student) conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information."[198] Therefore, use of an individual's identifiable "private information" can constitute human subject research even if there is no interaction with the individual himself.

(i) Private information is individually identifiable if the identity of the subject is or may readily be ascertained by the investigator or associated with the information."[199]

(ii) This definition is not as detailed as the enumerated data points constituting PHI under the Privacy Rule. However, if information is de-identified within the meaning of HIPAA, it should be sufficiently de-identified for the purposes of the Common Rule. The same might *not* be true in reverse.

(iii) Also, while sound arguments exists that a limited data set is not individually identifiable information under the Common Rule, the question is not formally settled and validation of that position by the IRB may be advisable.

b. While both the Common Rule and HIPAA apply to use of data in research if it is identifiable (each according to its own standard), the FDA Law does not take this approach. The FDA Law defines a human subject as "an individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may be either a healthy individual or a patient."[200] The definitions promulgated by the FDA do not make reference to

---

[195] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,710 (Dec. 28, 2000) (endorsing, as a disclosure risk reduction technique for de-identifying PHI, the use of methods to "limit[] the distribution of the records through a 'data use agreement' or 'restricted access agreement' in which the recipient agrees to limits on who can use/receive the data"); U.S. DEP'T OF HEALTH & HUMAN SERVS., *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, at 21 (Nov. 26, 2012), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (reiterating the endorsement of data use agreements and restricted access agreements as disclosure risk reduction techniques) (last visited June 14, 2016).

[196] "Federal Policy for the Protection of Human Subjects", 45 CFR§ 46(A)-(D).

[197] 21 CFR§ 50.1.

[198] 45 CFR § 46.102(f).

[199] 45 CFR § 46.102(f).

[200] 21 CFR § 56.102(e).

whether individually identifiable information is being used in deciding who is a human subject.

c. The recently promulgated amendments to the Common Rule (the "Final Rule") to the Federal Policy for the Protection of Human Subjects (the "Common Rule"), which has been adopted by HHS and 15 other federal departments and agencies that fund research. HHS' stated goals of these changes are to align the Common Rule with the modernization of the research and privacy landscape and to otherwise strengthen the Common Rule while reducing administrative burdens for researchers.

d. The Final Rule adopts a number of changes that will have a noticeable impact on the Common Rule's informed consent, waiver, and IRB review requirements. Many of the changes focus expressly on the privacy risk associated with use of identifiable data in research. While some of these changes may ease administrative burden on researchers, others (particularly the new informed consent and waiver requirements) may impose new challenges in pursuing secondary research. The particularly notable changes are as follows:

(i) While HHS did not adopt the controversial proposal to consider biospecimens that are unannotated with identifying data to be human subjects, the Final Rule requires HHS to periodically assess the Common Rule's identifiability standards, including whether the presence of genetic material embedded in biospecimens constitutes identifiable information, and permits HHS to update such standards through guidance.

(ii) The Final Rule imposes new informed consent form requirements. These requirements, including the requirement that consent forms disclose certain details regarding secondary use of data and biospecimens, obligate researchers to provide more specific information about the research study and potential future use than under the prior Common Rule.

(iii) The Final Rule also adds specific requirements for researchers who wish to obtain "broad" informed consent from subjects for the storage, maintenance, or secondary research use of identifiable private information or identifiable biospecimens. Though HHS's stated objective of this change is to provide enhanced flexibility to researchers, it is unclear whether it will minimize burden in a significant way compared to existing pathways existing under both current Common Rule regulations ("Pre-2018 Rule") and the Final Rule, such as waiver of informed consent.

(iv) The Final Rule revises and expands the categories of exempt research to include, among others, certain secondary research activities regulated under the Health Insurance Portability and Accountability Act ("HIPAA") and certain other secondary research activities. These changes meaningfully lessen the administrative burden researchers will bear when conducting secondary research that is regulated under HIPAA.

(v) The Final Rule streamlines requirements for study recruitment and screening activities.

(vi) The Final Rule includes revisions to the criteria for waiver or alteration of informed consent that may make it more challenging in some situations to obtain waiver or alteration of informed consent.

(vii) The Final Rule eliminates the authority of the Common Rule Agencies to oversee and enforce compliance with the Common Rule with regard to human subject research that is not federally funded or supported. Institutions may still choose to conduct such

research in accordance with the Common Rule; those who do should ensure that their internal oversight and compliance mechanisms align with this new framework.

K. Intellectual Property Challenges and Uncertainties

1. AI-enabled diagnostic support software has significant patentability issues in light of the decisions in *Mayo v. Prometheus Labs, Inc.*[201] and *Alice Corp Pty. Ltd. v. CLS Bank Int'l*[202]. These cases focus primarily on, and heightened the hurdle for the patent eligibility of subject matter, thus reinforcing the principle that ideas are not patentable and running those ideas through a computer does not make them patentable.[203]

a. In *Mayo Collaborative Servs. v. Prometheus Labs, Inc.*, the Supreme Court held that a methodology for giving drugs to patients and determining an appropriate dosage threshold based on the correlation between naturally occurring metabolites and therapeutic efficacy and toxicity is not patent eligible because the technology provided "instructions [that] add nothing specific to the laws of nature other than what is well-understood, routine, conventional activity, previously engaged in by those in the field.[204]

b. In *Alice Corp Pty. Ltd. v. CLS Bank Int'l*, the Supreme Court held that using computer software to implement an abstract goal (managing escrow debts) does not make the goal patentable. The Court enunciated a two-step test for subject matter patent eligibility: (i) determine whether the claims are directed to a patent-eligible concept (laws of nature, abstract ideas, and natural phenomena); and (ii) determine whether the claim's elements, considered both individually and as an ordered combination, transform the nature of the claims into a patent-eligible application.

2. Courts have already relied on *Mayo* and *Prometheus* as a basis for finding patent ineligibility of "revolutionary diagnostic technology."[205]

3. One potential argument in support of ineligibility is that AI is doing little more than churning out the same ideas that a practitioner could not patent.[206]

4. The feasibility of establishing and protecting other potential intellectual property protections such as copyright and trade secret will need to be addressed.

L. Billing and Reimbursement

Whether and to what extent AI-enabled diagnosis and treatment will be reimbursed by government and private payers remains uncharted territory.

1. AI-enabled diagnostic support software that are used similar to how diagnostic tests are used (i.e. ordered specifically for individual patients as confirmatory evidence for a suspected condition or

---

[201] 566 U.S. 66 (2012).
[202] 573 US 208 (2014).
[203] Tull, S.Y. and Miller P.E., "Patenting Artificial Intelligence: Issues of Obviousness, Inventorship, and Patent Eligibility," RAIL, The Journal of Robotics, Artificial Intelligence & Law, Volume 1, No. 5 (September – October 2018).
[204] *Id.at 69.*
[205] *Id. See, e.g., Ariosa Diagnostics, Inc. v. Sequenom, Inc*., in which the court found ineligibility of a novel method of prenatal diagnosis of fetal DNA. 788 F. 3d 1371, 1376, 1379 (Fed. Cir. 2015).
[206] Duke White Paper *supra* at note 1.

as a screening test for a defined population) have a clear pathway for coverage and payment, contingent on evidence of clinical usefulness (e.g. IDx-DR for diabetic retinopathy).[207]

2. AI-enabled diagnostic support software that has been integrated into EHR systems or other clinical workflows and meant to be used on every patient regardless of a physician's need may be viewed differently. Payors are less likely to pay individually for services provided to all patients.[208]

3. CMS Artificial Intelligence Outcomes Challenge

The Centers for Medicare & Medicaid Services ("**CMS**") launched a three-stage competition to accelerate AI solutions to better predict health outcomes such as unplanned hospital and skilled nursing facility admissions and adverse events for potential use by the Innovation Center in testing innovative payment and service delivery models.[209] The Challenge period began in March

a. Goals

CMS views the challenge as an opportunity for AI innovators to demonstrate how AI tools can be used to predict unplanned hospital and skilled nursing facility admissions and adverse events for potential use by the CMS Innovation Center in testing innovative payment and service delivery models. It prioritizes explainable intelligence solutions to help front-line clinicians understand and trust AI-driven data feedback to target scarce resources and improve the quality of care.

b. Structure

(i) Launch Stage: submission of application providing information about proposed solution to support selection as one of the 20 participants in Stage 1. (March 2019 through June 2019)

(ii) Stage 1: participants design and test proposed AI solution using certain Medicare claims data sets to qualify for participation in Stage 2. (Summer 2019 to Fall 2019)

(iii) Stage 2: participants may request additional claims data and refine solutions to earn the grand prize of $1.0 million or $250,000 second prize. (Winter 2019 through Spring 2020, with announcement of winners in April 2020)[210]

See Attachment D for a summary of other relevant laws and regulations.

V. ARTIFICIAL INTELLIGENCE COLLABORATIONS AND INVESTMENTS - PLANNING AND CONTRACTING CONSIDERATIONS AND STRATEGIES FOR BALANCING RISK AND OPPORTUNITY[211]

Health care related Artificial Intelligence technology and solution design, development and deployment initiatives will likely require participation and support of multiple players each of whom contributes a different but key ingredient for success and multiple agreements between and among them. AI's

---

[207] *Id.*
[208] *Id.*
[209] March 27, 2019 https://www.cms.gov/newsroom/fact-sheets/cms-artificial-intelligence-health-outcomes-challenge
[210] All dates are subject to change.
[211] This discussion is not intended as legal advice and should not be considered exhaustive of the full scope of relevant planning and contracting issues.

dependence on data of various types and from various sources that is robust and continually refreshed alone drives AI developers toward collaboration with providers, research institutions and others who provide a rich source of data.

The following is a discussion of key contracting and associated due diligence strategies for managing and allocating compliance and other enterprise risks in the context of data and other collaborations to pursue AI technology solutions initiatives. The discussion is not intended to cover all contexts or considerations. Further, some of the considerations discussed may be relevant with regard to some contexts but not others.

A. Structure, Integration and Coordination of Agreements

1. Phasing of AI Solution Development and Deployment

a. Some AI initiatives and the corresponding collaborations should be undertaken in phases. Starting with a proof of concept or pilot effort can provide an opportunity for further assessment of the feasibility of ultimate deployment of infant technology and avoid making a long-term investment and commitment of other resources that becomes unstainable and deflects the players from pursuing other opportunities. A phased approach may be more valuable in these respects with AI technology and solutions than with other digital health initiative.

b. If the initiative will be pursued in multiple phases over time, the relationship with the collaborators will evolve and change with the further development of the AI technology. Therefore, when contracting for the first phase to address to the extent possible key risk and success considerations relevant to those later stages for which it is important to lay an appropriate foundation, such as how the nature and extent of the activities, the roles and contributions of the parties, the outcomes/deliverables and the financial, legal and compliance risks are likely to change from phase to phase as the relationship evolves. The parties' relative negotiating positions/leverage on such key issues will likely be different for later stage negotiations. Choosing to delay addressing key later-stage issues at the earliest stages could cause delay or disruption by the need to "re-contract", failure to re-contract, and ultimate failure of the project.

2. Multi-Party Collaborations

Each agreement should contain a clear and complete description of the parties and their relative roles and responsibilities and how the agreement relates to the other agreements between and among the parties for the same collaboration, as well as a provision that obligates each player to fully cooperate with the others. This will provide for effective overall management of the endeavor and minimize the risk of confusion and/or "finger-pointing" and associated project disruption, delays and failures.

B. Key Data Related Considerations

The collection, sharing, aggregation, analysis and secondary use of vast amounts of data is certainly at the heart of any digital health innovation collaboration and no collaboration will be feasible or successful without that ingredient. However, such data dimensions raise a myriad of planning and contracting considerations. Key among them are the following.

1. Compliance with Privacy Rule's Prohibition on the Sale of PHI

The Privacy Rule expressly requires a covered entity or business associate to obtain an individual's authorization for the "sale of PHI" about the individual. This prohibition presents planning and contracting challenges for a digital health innovation collaboration and

could have a chilling effect on and participation in collaborative data initiatives. Regardless of whether the risk of a violation under a particular arrangement is low, medium or high, the potential for damage to the trust of physicians and patients and damage to overall reputation is a very real risk for AMCs.

a. The Privacy Rule defines the sale of PHI to mean a disclosure of PHI where the covered entity or business associate directly or indirectly receives remuneration, in cash or in kind, from (or on behalf of) the recipient of the PHI in exchange for the PHI unless the disclosure is for one of eight enumerated purposes, which include research and functions performed by Business Associates for covered entities (e.g., health care operations).

b. Note: A sale of PHI includes license and other arrangements granting access and use rights (as opposed to an outright sale).

c. A transfer of data for "research" or "health care operations" purposes is permitted but only if the covered entity or business associate receives remuneration that amounts to no more than the cost of arranging for or transferring the data. This narrow exception would limit the value, in cash and in kind, the covered entity receives in return for the data.

d. This limitation on remuneration creates challenges for a covered entity that contributes PHI to be used in the digital health development and deployment **particularly if the other collaborators retain the data and are given rights (exclusive or non-exclusive) to access and use the PHI for secondary purposes and the covered entity receives benefits** in the collaboration such as royalty free or discounted license/use rights to access and use a data bank created using the transferred data, an equity share in an entity created to commercialize a digital health product developed using the data (in whole or in part), free services of a technology vendor (e.g., cloud services), or the like.

    (i) How such benefits must be factored into the determination of the "appropriate cost-based limitations on remuneration" remains unclear and some or all of such benefits may be difficult to value and document with objective, reliable valuation methodologies and data.

    (ii) Nonetheless, the planning and contracting efforts must separately identify and analyze each and every benefit derived and contribution made (in cash or in kind (e.g., contribution of clinical or research expertise, data license/access rights)) by each of the covered entity and its collaborators in the digital health collaboration for which the covered entity transfers PHI, using commercially reasonable and prudent, good faith efforts.

    (iii) The covered entity should also consider whether the economic terms of other agreements/relationships it has with any of the collaborators in a digital health collaboration could be characterized as indirect remuneration for the PHI contributed in the digital health collaboration. (Note, however, that, in connection with the development of the HIPAA sale of data regulations, HHS confirmed that bona-fide, reasonable compensation paid by a sponsor to a covered entity in connection with a sponsored research study will not be considered remuneration for data in violation of the sale of PHI because the payment is for conducting the research not for the data the covered entity transmits to the sponsor on case report forms in connection with the study).

(iv) The collaboration agreement should clearly and precisely document the economic terms of the agreement relating to those contributions and benefits. If the value of the covered entity's benefits exceed its contributions, a sale of PHI violation will likely arise unless the only data contributed is data that is de-identified in accordance with the HIPAA de-identification standards.

e. Even a limited data set is subject to the Sale of PHI prohibition because it is not fully de-identified.

f. However, license or sale of data that meets the HIPAA de-identification standard would not violate the sale of PHI prohibition.

(i) In some cases, de-identification based on elimination of all 18 identifiers ("safe harbor method") could diminish the value of the data for the intended uses in the development effort.

(ii) In any case, as discussed further below, that safe-harbor method of de-identification may become infeasible in some cases if the de-identified PHI contributed will ultimately be combined with data from a number of other sources, both identifiable and de-identified, that includes unstructured data, consumer generated data and data from other sources, either for purposes of the collaboration or by one of the collaborators for its own purposes under rights it is given to use the de-identified data for secondary purposes. (See discussion of De-Identification challenges below.) In such case, the statistical certification path for de-identification provided in the HIPAA regulations may be the more viable and reliable alternative to avoiding a violation of the prohibition.

(iii) Under either de-identification method, a key consideration whether the de-identification will be done by the covered entity before transferring the data or by one of the other participants in the collaboration. If the latter:

(a) An Honest Broker arrangement will be required to accomplish the de-identification The Honest Broker compliance strategy creates additional challenges if the same entity is both the researcher and the Honest Broker. In such case, physical, electronic and administrative (policies and procedures) firewalls must be established between the personnel conducting the de-identification and the personnel using the de-identified data to conduct the research and, if re-identification is later needed, it may be done only by the personnel who did the de-identifying and a consent, authorization or IRB of waiver thereof may be needed if the re-identification is to support the conduct further research; and

(b) The Covered Entity providing the data should also preserve the right to direct which de-identification method.

2. Special De-Identification Challenges in the AI Context

a. Feasibility of De-Identification in the Context of AI Technology and Solutions

(i) Achieving adequate de-identification has become more challenging in the context of today's increasingly complex and sophisticated electronic/virtual data "ecosystem."

(a) Algorithm developers need to assemble data from multiple sources to train machine learning algorithms. Therefore, data supporting AI development and use is often derived from a data warehouse that is robust, multi-dimensional and intended for a broad range of future uses.

(b) The data integrated into the warehouse: (i) comes in various forms (including different structured forms, different curated forms, unstructured data from various public sources (e.g., literature such as professional journals, patient/consumer mobile devices), and/or (ii) comes from various sources (e.g., other research and development partners, other covered entities, other data warehouses, patients/consumers directly or through wearables and mobile devices, from social media and third party data repositories).

(c) Information collected by non-covered entities (e.g., Google, Apple, data aggregators) is not governed by the HIPAA Privacy Rule; nor is HIPAA applicable to social media platforms, smart phone apps, life insurers, retailers, credit-card companies, and Internet search engines. (Parasidis, *A Belmont Report for Health Data*, 380 NEJM 1493 (April 18, 2019).

(ii) A study conducted by Berkeley engineer, Anil Aswani, and his team conducted and published in December 2018, found that use of artificial intelligence to link identity to health data by analyzing daily step patterns using data collected consumer wearables (e.g., activity trackers, smartwatches, and smartphones) that was previously de-identified under current de-identification standards and correlating that data to de-identified demographic data,[212] and that even stripping all data identifiers did not protect against re-identification.

(iii) Accordingly, it is becoming increasingly challenging to demonstrate under the HIPAA De-Identification Safe Harbor (i.e., removal of the 18 identifiers) that the covered entity 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."

(a) Therefore, the "safe harbor" pathway of removing the 18 identifiers is increasingly being found inadequate especially in the AI innovation context.

(b) Therefore, more sophisticated and well-tested de-identification methods/techniques that qualify for the "statistical certification" pathway is becoming the more reliable alternative. Available experts are limited in number and increasingly in demand. Therefore, a covered entity may wish to develop or harness the ability internally to perform the statistical de-identification.

(iv) The "black box" dimensions of AI technology and solutions add meaningfully to this growing uncertainty with regard to de-identification.

(v) De-identification of data can neutralize important information, including geographic, socioeconomic, and other social determinants of health and

[212] Na, L., Yang, C, *et al.,* "Feasibility of Reidentifying Individuals in Large National Physical Activity Data Sets From Which Protected Health Information Has Been Removed With Use of Machine Learning," JAMA Open Network (December 21, 2018), *available at* https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2719130

diminish the utility and value of the data for use in AI innovations. De-identification can also diminish the AI's effectiveness by "making it difficult for the program to match data from different databases …"[213]

(vi) There is also concern that de-identification can introduce bias into the data.

(vii) Use of Synthetic Data

(a) Synthetic Data Sets are generated from existing datasets and maintain the statistical properties of the original dataset.

(b) Rows of observations in synthetic data sets do not correspond to identifiable individuals from the original data set. Thus, synthetic data derivatives of identifiable data are quantitatively identical to the source data but cannot be linked to the individuals from whom the source data was derived,214 and some computer scientists have concluded that, while not a cure all, synthetic datasets are a "privacy-conscious alternative to raw data" and should be accepted by the privacy community as a valid, next step to the database privacy problem.215

(c) Synthetic data has limitations for analytical purposes. For example, synthetic data may replicate certain general trends of the original dataset, but may not necessarily be able to predict specific trends within a dataset (e.g., all-cause death v. cardiovascular death. There is also no consensus about how best to create synthetic datasets. [216]

(viii) Who undertakes the De-identification

A Covered Entity may use either its own workforce or a business associate to do the de-identification work as part of its "healthcare operations."[217] Special considerations need to be addressed to manage the HIPAA compliance risk when a business associate will do the de-identifying.

(ix) Very often, the business associate is the same person or entity that will use the de-identified data. If so, the Business Associate Agreement must obligate the business associate to return or destroy the identifiers, and any key or code that could be used to re-identify the data, once the de-identified data set has been created."[218]

(x) If it is important for the business associate to retain the PHI or re-identifying code, an "Honest Broker" arrangement can be established by implementing a firewall (technical and administrative) between the personnel doing the de-identification and the personnel who will use the de-identified data in connection with the collaboration that is sufficient to prevent the personnel

[213] Duke White Paper *supra* at note 1.
[214] Foraker, R., Mann, D., "Are Synthetic Data Derivatives the Future of Translational Medicine?" American College of Cardiology Foundation, JACC: Basic to Translational Science Vol. 3, No. 5 (2018), *available at* http://basictranslational.onlinejacc.org/content/3/5/716
[215] Bellovin, S., Dutta, P., and Reitinger, N., "Privacy and Synthetic Datasets," 22 STAN. TECH. L. REV. 1 (2019), *available at* https://law.stanford.edu/wp-content/uploads/2019/01/Bellovin_20190129-1.pdf
[216] *Id.*
[217] 45 C.F.R. § 164.50.
[218] Department of Health and Human Services, "Health Services Research and the HIPAA Privacy Rule," p. 11.

who will use the data from gaining access to the PHI or re-identification codes.

(xi) Whether and to what extent the data recipient will be permitted to use the PHI provided for one purpose for a secondary purpose should be addressed at the outset and if the recipient and the Business Associate doing the de-identification are the same entity, special Honest Broker protections will be needed and sale of data prohibition compliance needs to be considered. (See Sale of Data discussion herein.)

(xii) The planning and contracting process should address and document: (a) whether covered entity's PHI will be needed for the collaboration; (b) whether the covered entity will de-identify the PHI internally or rely on the collaborator or an independent third party; (c) if the covered entity will rely on the collaborator, what de-identification method will be used and, if statistical certification is required, who will be retained, on what the terms, what input will the covered entity have on those terms (particularly the form and content of the statistical opinion), who will bear the cost, and who will be entitled to copies of the opinion.

(xiii) Be alert for confusion between a "de-identified" data set and a "Limited Data Set". A Limited Data Set contains PHI, is not De-Identified Data and can be used only for limited purposes and under prescribed terms of a Data Use Agreement. This is a common trap because the term "de-identification" may mean different things to different parties and be misunderstood by an unregulated collaboration participant.

3. Business Associate Agreement Considerations

a. Direct HIPAA Privacy and Security Compliance Obligations of Business Associates

(i) Particularly in light of the expanded definition of Business Associate in the final HITECH Act regulations, Third Party HIT Vendors, HIT Support Organizations (including Data Aggregators, Data Analytics providers, and Cloud Computing Vendors), Health Information Exchanges, Accountable Care Organizations will typically be considered a Business Associate under HIPAA.

(ii) The HITECH Act provisions hold a business associate and its subcontractors directly responsible for HIPAA privacy and security compliance requirements. (See related limitation/disclaimer liability discussion below.)

(a) Section 13401 of the HITECH Act provides that certain provisions of the HIPAA Security Rule will apply directly to business associates -- specifically, those provisions relating to: (1) administrative safeguards,[219] (2) physical safeguards,[220] (3) technical safeguards,[221] and (4) policies and procedures and documentation requirements.[222]

[219] 45 CFR § 164.308.
[220] 45 CFR § 164.310.
[221] 45 CFR § 164.312.
[222] 45 CFR § 164.316.

(b) Section 13404 of the HITECH Act provides that certain provisions of the HIPAA Privacy Rule will apply directly to business associates -- specifically, those provisions relating to: (i) uses and disclosures of PHI,[223] and (ii) business associate contract requirements (45 CFR § 164.504(e)).

(c) Section 13402 of the HITECH Act makes a business associate directly liable for notifying the covered entity upon discovery of a breach of unsecured PHI.

(iii) Therefore, Business Associates must adopt and implement all HIPAA-required privacy and security policies and otherwise comply with the above-listed HIPAA-required privacy and security standards and requirements.

(a) A Covered Entity should conduct early due diligence to determine that the Business Associate and its subcontractors have in place adequate policies, procedures and infrastructure to meet its obligations. This should include, among other things, examination of whether sufficient security infrastructure is in place with regard to "Data in Motion" and "Data at Rest" to qualify the PHI being contributed, accessed and exchanged as secure rather than unsecured PHI so as to avoid the data breach notification and reporting requirements under the HITECH Act and Final Rule. This is particularly important in the case of a BA that has little or no experience in handling healthcare data under U.S. privacy and security laws or a BA that has limited scalability and resources.

b. Contractual Obligations

Such direct compliance obligations do not fully protect the covered entity and thus do not eliminate the need to contractually address privacy and security obligations of parties to the collaboration who will perform the role of a Business Associate such as date a breach reporting and scope of liability for data breaches and other performance failures.

c. Data Breach Considerations

The BAA should include time frames for providing such notification that allow the Covered Entity sufficient time to comply with its notice and reporting obligations after **receiving** the report of the breach from the BA.

(i) Liability Limitations and Disclaimers

(a) Various types of harm resulting from data breaches and other violations of HIPAA and the HITECH Act (as well as other federal and state privacy, confidentiality laws and data breach notification laws) (e.g., injury to patients, penalties and fines, and internal costs incurred to meet notification requirements and implement other remediation steps), particularly harm resulting from data breaches, will likely fall into one or more of the damage categories addressed in typical vendor liability limitations and disclaimers (e.g., caps on direct damages and disclaimers of all liability for consequential, incidental and special damages). The Business Associate Agreement should be carefully drafted to establish the appropriate allocation

[223] 45 CFR § 164.502.

of risk for these types of harm, and associated vendor indemnification obligations.

(b) The BA's direct exposure to OCR sanctions for its failure to comply with its direct obligation under HIPAA should not be considered adequate protection of the Covered Entity against such a failure or a failure to comply with its contractual obligations to the Covered Entity (e.g., the breach notification requirements). Rather, the BAA should also expressly provide for reimbursement of, or indemnification for, expenses and damages incurred by the Covered Entity as a result of the BA's failure to fulfill its obligations either under HIPAA itself or to the Covered Entity under the BAA.

(c) The Business Associate's willingness to indemnify or otherwise assume liability for third party claims (either unlimited or with a super cap) often various depending on several key factors: (i) the size of the Business Associate; (ii) the size and importance of the customer; (iii) the type of services being offered (e.g., enterprise or the standard "$40 per month account"); (iv) the size of the deal; and (v) the customer's security obligations and policies, with the idea that cloud service providers will be more willing to take on some liability if the customer is also taking affirmative steps to prevent security issues. [224]

(d) Business Associates should assume greater liability exposure when hosting data/data warehouse that supports the customers' principal enterprise (e.g., hosting a provider's EMR system, hosting a payor's claims processing system, hosting an enterprise-wide data warehouse) as opposed to hosting a copy of a portion of a customer's enterprise data for a more limited purpose (e.g., to provide data analytics services or support the customer's ability to do data analytics).

(e) Business Associates should assume greater liability exposure, even when only hosting a copy of a portion of a customer's enterprise data, if, in addition to hosting/using it to support the customer's operations, it seeks rights to use the data for its own operations, to enhance of its existing products/solutions or development of new ones, and for other secondary use purposes.

(f) Strict liability for the "sophisticated hacker" incidents should be a shared risk for which both parties maintain adequate insurance

(g) No industry standard exists for determining the damages caps for data breaches. The following considerations provide guidance for the parties in determining whether to agree to a super cap on data breach liability: (a) the total value of the contract; (b) the maximum amount of insurance coverage available to cover data breaches (both the service provider's and the customers) and applicable coverage exclusions; (c) expected term of the agreement; (f) quantity of data covered under the confidentiality or security provisions; (g) the geographic origin of the data covered under the confidentiality or security provisions (e.g., PII originating from Europe); (h)

[224] *Cloud Computing 2013: Cut Through the Fluff & Tackle the Critical Stuff – Contract Issues*, PRACTISING LAW INSTITUTE (June 24, 2013), http://www.pli.edu/Content/OnDemand/Cloud_Computing_2013_Cut_Through_the_Fluff/_/N-4nZ1z12oy5?ID=158223 (last visited June 14, 2016).

other applicable risk profile factors (e.g., how long the provider and customer have been in business and market share); and whether the Business Associate is permitted to de-identify and use the data for secondary purposes..

(h) Another consideration to factor into a determination of a cap is the amount of recent settlements of government investigations/enforcement actions relating to security breach incidents.[225]

[225] *See* http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html for a complete listing of OCR Settlements and Civil Monetary Penalties (last visited June 14, 2016).

4. Data Ownership

a. In today's "Big Data" driven world, data and its derivatives are now considered a valuable business asset that can command a high price tag. However, **w**idespread disagreement exists regarding ownership of data and intellectual property rights associated with and derived from data repositories and warehouses.

(i) Claiming intellectual property protection for raw data is difficult because raw data is factual information that lacks the level of originality necessary to merit protection under copyright law. Individual data elements are generally only protectable by maintaining confidentiality or by placing contractual restrictions on reuse and distribution.

(ii) However, aggregated data and the ability to run various analytics has considerable value, well beyond the value of any individual data point. Therefore, protection of data as a compilation may be available under copyright law if the data is selected, coordinated, or arranged in an original manner. For example, the raw data regarding the weather on January 1, 2016, in New York, New York (e.g., temperature and wind speed) is not protectable, but when combined with other data points in a specific geographic region and time period in an analysis offered to healthcare providers to predict when the common cold might be most prevalent, the compilation of data and any resulting predictive analysis may be protectable under copyright law.

b. Nonetheless, **t**his ownership question becomes prominent as a result of the "big data" cornerstone of most digital health collaborations, particularly with regard to dimensions such as creation of robust, valuable repositories that serve the collaboration's development and commercialization efforts, but can also be valuable for uses by the collaborators and third parties for purposes beyond those of the collaboration[226] As the law evolves and the debate continues, therefore, participants in digital health collaborations should consider "contracting around" this ownership and intellectual property issue using confidentiality and data access and use rights provisions, including secondary use rights provisions such as those described below, to claim and protect what the value of data so as to avoid disputes down the road.

5. Secondary Use Rights

Collaboration participants, whether or not serving as Business Associates of a covered entity participant, typically have a keen interest in using data they receive in the context of a collaboration for secondary purposes beyond those of the collaboration (e.g., future product development, testing and marketing of solutions other than the one that is the subject of the collaboration; building and enhancing robust data repositories to be exploited for a profit (including license or sale of data to third parties)).

a. The collaboration agreements should explicitly address the nature and extent of any secondary use rights that address key consideration such as the scope of permitted use (including whether the collaborator may undertake de-identification of the data and then use the de-identified data for secondary purposes), restrictions on use, and

[226] Case law and state statutes governing tissue donation also implicate information exchange networks and information repositories both with respect to the need for individuals' informed consent and the preservation and allocation of ownership and use rights in agreements between and among the parties involved in an electronic information exchange or data repository. *See, e.g.,* Washington Univ. v. Catalona, 552 U.S. 1166 (2008).

associated consent/authorization and other regulatory compliance requirements applicable to permitted use of identifiable data.

b. Participants who are willing to grant secondary use rights to fellow collaborators should remain aware of the prohibition on a covered entity's sale of PHI.

c. A participant who is interested in granting legally permissible secondary use rights should articulate restrictions such as exclusion of certain categories of data it contributed and prohibitions against exploiting the data for profit by licensing or selling it to a third party that competes with the participant granting the secondary use rights and/or the collaboration's endeavor or spin-off.

d. Remuneration (other than reimbursement of cost) for granting a collaborator rights to use de-identified data of a participant is permitted under HIPAA as de-identified data is not subject to the sale of data prohibition. (Note, however: Non-HIPAA driven restrictions on remuneration for de-identified data or tissue might exist in an organization's internal policies and procedures or the terms of consents that commit to secondary use protections than required under applicable law.)

   (i) The nature and extent of the remuneration for data rights will vary depending on the nature of the collaboration, the data, and other contributions of value made by the participant (e.g., contribution of clinical or research expertise needed to support the development effort).

   (ii) The remuneration may include one or a combination of license fees, service fees, a royalty interest in a revenue stream generated by the collaborators' secondary use of the data, an equity interest in an entity that commercializes and exploits the data and/or a digital health solution created through the secondary use of the data, and free rights to access and use a repository the collaborator created in part through use of the secondary data.

e. A participant should also consider all sources of data they intend to contribute to the collaboration and include in a grant of secondary use rights and ensure that appropriate rights are in place at each step of the chain of transfer. In particular, the participant must avoid granting digital health collaborators secondary use rights to data the participant contributes to the collaboration that would conflict with its contractual rights to third parties such as third parties whose data is included in the data the participant contributed and third parties to which the participant has also contributed the same data for primary or secondary uses. Granting a collaborator "exclusive" secondary use rights could create such a conflict.

f. Covered Entities seeking to preclude the creation and secondary use of PHI (including use to create and make secondary use of de-identified data), should include affirmative prohibitions and avoid conflicting provisions in the agreement. See Attachment E for an example of such affirmative contractual parameters/restrictions.

g. In addition to the privacy-related provisions concerning permitted or prohibited uses, confidentiality and intellectual property clauses should be carefully reviewed and drafted so as to avoid conflicts and inconsistencies between secondary data use rights and intellectual property rights such as ownership and licenses of copyrights and trade secrets and the definition of and restrictions on use and disclosure of confidential information. Defects in such secondary use rights provisions may unintentionally open the door on the one hand, or create a barrier on the other hand,

to exploiting big data for secondary purposes and can significantly undermine the financial value and safeguards of the underlying data.

h. Exchanging and combining data from a broad variety of sources, in a variety of forms (structure and unstructured), and through a variety of electronic channels can also lead to unanticipated uses of the data by a collaborator given secondary use rights such as profiling of consumers in ways that can be harmful and overly-intrusive personalized advertising that should be considered when crafting the terms of the agreement relating to the scope of and restrictions on secondary uses.

6. Data Accuracy, Integrity and Completeness

Collaboration agreements should expressly articulate the relative responsibility of the parties for data accuracy, integrity and completeness with regard to data contributed to the initiative and the data created and used to support the initiative. Many of the same considerations discussed above with regard to the difficulties of de identifying data create the need for special focus on data integrity considerations (e.g., inclusion of unstructured data, data from multiple sources and in multiple forms, aggregating data from different repositories, and inclusion of consumer/patient generated data). Data integrity challenges and associate risks will likely increase commensurate with increased exploitation of the data in the context of both the collaboration and the secondary uses.

7. Exit Strategy – Return or destruction of Data

a. Return or destruction of a participant's data once aggregated in a repository may be possible with minimal disruption if a copy of that data is maintained in its originally-submitted form and content in a file that is segregated from the aggregated data. In this regard, the contract should be clear that, as between the participant and the repository owner, segregated data is at all times owned exclusively by the repository participant, even if the segregated file in which it is stored is hosted by the repository owner or a third party on behalf of the repository owner.

b. In many (if not all) cases, the data incorporated into a repository in connection with the collaboration is merely a copy of data the participant continues to maintain in its own EHR or other electronic record systems. In such case, the participant arguably is not harmed or disadvantaged if the repository does not return the data.

c. To avoid disruption and deterioration of a robust data repository, the parties should consider establishing a participant "data tail" obligation following termination of or withdrawal from participation. This can be controversial and something participants may resist, but it is particularly important if the repository has been used to support research studies that are still ongoing following the termination or withdrawal.

8. General Due Diligence and Contracting to Address Key Data Considerations

Following is a list of questions for use in conducting the due diligence and crafting contract provisions to identify, allocate and manage the risks associated with the data considerations discussed above, many of which are driven largely, but not exclusively, by privacy and security considerations.

a. Which stakeholders will provide, access, exchange the information?

b. What data will be contributed exchanged?

(i) Will it contain "identifying" information when contributed by a participant?

(ii) Will it contain "identifying" information when used/accessed by participants?

(iii) Will the data contain types of information subject to special protections under laws other than HIPAA/HITECH?

(iv) Will any competitively sensitive information of competitors be involved?

(v) What was the original purpose for which data was contributed/exchanged?

(vi) Will the data come in various non-standardized forms? Structured or Unstructured? Patient-Consumer generated data? Will it be combined with data in various forms and from various sources?

(vii) Is any supporting technology coming from third party vendors?

c. Are any secondary uses contemplated/permitted? If so:

(i) What was the original purpose for which data was contributed/exchanged?

(ii) Was the secondary use contemplated at the time the data was originally gathered?

(iii) Was more data gathered than necessary for the original purpose? Did the consent/authorization cover those purposes?

(iv) Was a consent/authorization obtained and what purposes/uses did it cover? If no consent was obtained, was there a waiver, authorization/consent or other compliance pathway permitting the use?

(v) Will the data be de-identified, or a limited data set derived from it, prior to using the data for secondary purposes?

(vi) Will data be drawn from various sources?

(vii) Will data of other types and from various sources be aggregated into a centralized repository or be maintained and accessed on a decentralized basis? If so, what other types and sources (e.g., structured, unstructured, consumer generated, literature)

(viii) Will the data be made available to other than those who contribute data to the arrangement?

(ix) Will any of the participants in the arrangement pay or receive remuneration to or from other participants? If so, what is the amount of such remuneration and how is it determined? How does it compare to the cost incurred to contribute information to the arrangement?

(x) Will the infrastructure depend in whole or in part, in the short term or long-term, on the support of third parties offering a complete turnkey arrangement or just certain infrastructure, such as cloud computing or other server capability that will facilitate the exchange of information without the need for myriad source-to source interfaces). If so, will there be any downstream vendors/support organizations? Where are such third parties located?

d. If the data will be stored and/or analyzed on a cloud, provided by a collaborator or third party vendor, where are the servers and the personnel supporting them – U.S. or

Off Shore, and will the cloud be a multi-tenant cloud? If the latter, how will the AMC's data be segregated and safeguarded?

(i) Required Contractual Protections and Parameters

(a) The data governance criteria and guidelines should also specify any minimum required contract protections for different types of data collaborations.

(b) Such protections would address many of the topics addressed elsewhere in this outline (e.g., Business Associate Agreement requirements, restrictions on access and use rights (particularly data ownership and license rights, right to de-identify and associated standards, secondary use), legal and regulatory compliance representations and covenants, data breach response and remedies, indemnification, limitations and disclaimers of liability and exclusions from same)

(c) Another category of required contractual protections is the inclusion of special privacy and security safeguards necessitated by certain types of collaborations over and above those that may be prescribed by law or a Business Associate Agreement.

(1) For example, in a collaboration in which a third party recipient of the data will both de-identify the data, exploit the de-identified data for secondary purposes, and retain the identifiable data or key/codes that can be used to re-identify, it will be important to specify additional protections such as detailed, technology infrastructure and electronic communication requirements, written "Role-Based Access Controls" and other "Firewall" protections against the impermissible access and use of the identifiable data from which the de-identified data was created by those who will use the de-identified, commitment not to attempt to re-identify the data and to ensure that any third party contractors of the recipient do not attempt to do so. If the recipient does not need to retain the identifiable data, key or codes, of course the ideal is to require return/destruction of identifiable data and all keys/codes that could be used to re-identify the data.

(2) Such additional protections should be further secured by including a right to conduct inspections of the recipient's compliance with all the privacy and security standards and extra requirements under the agreement.

9. Information Blocking

The collaboration agreement should address the potential for blocking by one or more of the participants of access to PHI collected and used in connection with the collaboration that could violate applicable law, including HIPAA and the 21st Century Cures Act. Note, information blocking that does not violate law but is contrary to the business needs and interests of a participant also must be addressed.

a. A business associate's general obligation under the HIPAA Security Rule to ensure the confidentiality, integrity and availability of PHI that it creates, receives, maintains or transmits on behalf of a covered entity. "Availability" means that data or information is accessible and useable upon demand by an authorized person. A Business Associate that blocks a covered entity Customer's access to essential PHI potentially violates the Security Rule's "availability" requirement. Maintaining the availability of PHI also includes returning PHI at the termination of an agreement to a Customer in a format that

is reasonable in light of the Vendor's obligations under a business associate agreement. Health IT Solutions arrangements involving collection, aggregation and analysis of PHI that do not require the covered entity to be able to access the source PHI or a repository created using it and do not require return of the source data after it is no longer needed by the collaborator would not implicate the information blocking prohibition.

b. A covered entity Customer in turn has an obligation to ensure the availability of its own information and may be in violation of both the Privacy Rule and the Security Rule provisions relating to business associate arrangements if it enters into a business associate agreement (or terms in the underlying agreement) that by its terms prevents the Customer from fulfilling this obligation.

c. The 21st Century Cures Act established new civil monetary penalties of up to $1 million per information blocking violation, including potential penalties for false attestations by health information technology vendors. The law instructs ONC to define the practice and outline "reasonable and necessary activities that would not constitute information blocking. OIG is already reviewing cases, and is preparing to take action against prospective violators under its new authority.[227]

10. Privacy and Security Compliance Capabilities of the Infrastructure Supporting the AI Solution

a. Evaluation/Due Diligence

An essential question is, but is not limited to, whether the security infrastructure supporting the AI solution and the collection, storage and transfer of data on which it depends can: (i) establish and manage access rights according to role and purpose of access (e.g., treatment, billing and payment, health care operations (e.g., utilization review and quality assurance, research) and utilize multi-factor user authentication; (ii) limit access to certain records or types of data (e.g., records of patients who have refused or withdrawn consent, categories of information given special protection under federal and state laws); (iii) segregate/firewall sensitive data/other data (e.g., data relating to care for which a patient pays personally and requests not to be disclosed to a health plan) for which consent to disclosure has been withheld or not yet obtained; (iv) monitor and audit access; (v) encrypt data in motion and at rest; and (vi) require the use of complex passwords.

b. Contract Provisions

The collaboration or investment agreements should include provisions tailored to the findings during the due diligence/evaluation process.

(i) The contract should include a detailed description of the applicable security infrastructure, and require ongoing updates and assessments.

(ii) It may be impossible at the time of initial contracting to anticipate all relevant business and compliance considerations that could affect the essential features and functions of the system over its useful life. Regulatory changes as well as operational/business process changes will likely occur, and such changes may necessitate system modifications, enhancements, retrofitting or other measures.

[227] David Pittman, "HHS Gearing Up For Info Blocking Cases," Politico (November 1, 2017), *available at* https://www.politico.com/tipsheets/morning-ehealth/2017/11/01/analysis-of-helps-health-it-hearing-223116

Therefore, the contract should address the obligation of the vendor to make necessary system changes and at what cost.

c. Special Considerations in Cloud Computing Agreements

The use of Cloud Computing in support of a digital Health IT solution by its very nature involves contracting with one or more third party support organizations, including perhaps one of the collaborators.

(i) One key consideration is whether all or a portion of the infrastructure will used to service more than one tenant of the cloud and whether all or a portion of it will be segregated/partitioned (physically or virtually) for particular tenants. For example, a vendor may use the same infrastructure to service one or more tenants, but will not store one tenant's data with the data of another tenant in the same segment of the cloud infrastructure.

(ii) Another consideration is whether all servers and support personnel will be located in the U.S. (See above discussion of off-shore data exchange prohibitions.

(iii) Yet another consideration is whether third party technology and support will be used behind the scenes so to speak and whether those third party vendors can and are obligated to meet the requirements of the primary vendor with regard to data privacy, integrity and location of servers.

See Attachment E for a contractual provision that addresses these and other important privacy compliance issues.

11. Compliance Obligations of the Parties

a. Affirmatively obligating all collaboration partners to comply with their own direct obligations under applicable law is standard and of course essential.

b. In the case of a collaborator who is a tech company providing technology and/or support services to an AMC in support of the collaboration, however, that general compliance obligation is distinguishable from a covenant, representation and warranty that the technology and services the tech company is providing will support the AMC's ability to meet its own legal and regulatory privacy and security compliance obligations, both as they exist currently and going forward. Special contract language is needed to address this distinction in the agreement. Be cautious of representations that technology is "HIPAA-Compliant" as that can mean different things to a vendor than to a covered entity and fall short of what a covered entity needs to meet its HIPAA compliance burden.[228]

[228] *See* Christina Farr, "Amazon Alexa is missing one big thing before it gets into healthcare," *available at* https://www.cnbc.com/2017/09/25/amazon-alexa-not-yet-hipaa-compliant.html, reporting on Amazon's public disclosure that Alexa is not yet ready for healthcare because it is not "HIPAA-compliant" and thus not ready for uses such as recording patients' lab results or other types of identifiable health information in a clinical setting.

12. Cross Border Data Transfers

a. EU Global Data Protection Regulations (GDPR)

On May 25, 2018, the GDPR will become immediately effective and enforceable and will be the primary EU[229] law regulating the collection, use, safeguarding and disclosure of "any information relating to an identified or identifiable natural person" (*i.e.* a Data Subject) ("PII"), including, without limitation, PII that fits within "special categories of personal data" that, by their nature, are particularly sensitive ("SPDs). The GDPR replaces the EU Data Protection Directive 95/46/EC and is designed to update and harmonize data privacy laws across the EU to protect and empower individuals in the EU, and to reshape the way organizations with operations or customers in the region approach data privacy. See Attachment D for a brief overview of the GDPR.

b. Offshore Data Access and Processing

Organizations should consider whether to incorporate provisions addressing cross-border concerns, particularly when dealing with foreign vendors or arranging for the provision of services by a Business Associate (or, in turn, downstream Business Associates) located outside the U.S. or with personnel based outside the U.S. The cloud contract should specify the location of the data centers to be used for storage of PHI and other information and of the personnel who will access the data. If use of overseas data centers is permitted, the privacy policy provided to patients should indicate that their information may be transferred outside the U.S.

C. Intellectual Property (IP) Rights

The following potential IP rights opportunities and challenges can arise both in the early stages of a collaboration or commercialization effort and throughout the entirety of the potential life cycle of the innovation.

1. The following are key planning and contracting considerations that should be specifically addressed early in the formation stages and in the collaboration agreement.: (a) whether and to what extent the collaboration will involve use of the collaborators existing IP, (b) whether the collaboration will spawn IP through the individual efforts of one of the parties or the joint efforts of all of the parties, or of their clinicians and other professionals;[230] (c) whether that new IP was derived in whole or in part from one or more of the parties' original IP; (d) what licenses and cross-licenses are needed to enable the parties to use one another's original IP; (e) who will own the IP developed in connection with the collaboration and whether those ownership rights will vary depending upon which parties developed it and whether it was derived from any of the parties' original IP.

2. Each type of potential IP should be separately identified and addressed (e.g., data, algorithms, tools, data compilations, trade secrets, trade names, etc.).

3. Exclusive rights, rights of first refusal, and options of the parties to participate in commercialization or other exploitation of IP spawned by the venture, any remuneration to be

[229] As of December 22, 2017, the Members of the European Union include: Germany, Poland, the UK, Croatia, France, Spain, Italy, Romania, Sweden, Greece, Bulgaria, Czech Republic, Hungary, Austria, Netherlands, Finland, Belgium, Slovenia, Lithuania, Luxembourg, Portugal, Denmark, Malta, the Republic of Ireland, Estonia, Slovakia, Cyprus, and Latvia.

[230] *See* Jeremy C. Fox, "US District Judge Rules Dana-Farber Researchers Helped to Invent Landmark Cancer Treatment," Boston Globe (May 18, 2019) *available at* https://www.bostonglobe.com/metro/2019/05/18/dana-farber-researcher-ruled-inventor-cancer-treatment/IgNlGfl2epmJv4z0ucEDqI/story.html

paid for those rights, and any key economic terms relating to such participation should be specified.

4. Evaluating and Selecting Home Grown IP's Commercialization Opportunities

Invention Disclosure Forms should be promptly and carefully reviewed for inventions with potential for commercialization, keeping in mind the need to balance the sometimes competing objective of commercializing promising technologies and further the institution's overall mission, vision and purpose. The Forms should require disclosure of whether the inventor involved any third party in the development of the discovery or has discussed the invention with any third party.

a. That review should be completed in the first instance by individuals/oversight bodies who are free of conflicts of interest arising from current interests held by the institution, individuals or their family members, employers or other business interests or their interests in investing in the commercialization initiative.

b. If the evaluation process concludes that the technology discovery presents commercialization promise, the institution should immediately take all steps necessary to validate and protect its intellectual property rights and promptly thereafter appoint a disinterested individual to shepherd the invention through the next steps in the commercialization process.

c. A key consideration in validation of the institution's IP rights and its ability to grant licenses to the IP is whether the IP emerged from any research and development projects funded by government or private grants with terms that claim ownership by the funding organization and/or requirements for approval for and other restrictions on the institution's ability to transfer.

d. To ensure the institution receives maximum value for its IP, the next key step is determining whether there is a business case for commercializing the invention and whether that should be done through a spin-off entity created by the Captive Investment Entity or through another innovation fund or portfolio company and for licensing the IP directly to the entity that pursues the commercialization. That "business case" analysis should be done using generally accepted valuation methods, with independent oversight, and be well documented, as should the basis for the ultimate decision to pursue one commercialization strategy as opposed to another.

e. Thereafter, the management and/or board committee responsible for oversight of the AI Innovation investment can play an important role in the further evaluation and valuation of the IP license and overall commercialization opportunity.

f. Individuals with current interests and relationships, or direct or indirect interest in investing in the commercialization venture, should be involved if at all only in an advisory capacity and with the overlay of ongoing independent oversight within both the institution and the Fund Entity and final approval by the independent committee of the Creator of the Captive Investment Entity.

g. No consultation with any individuals or entities interested in investing should occur until IP rights have been secured, the initial business case has been developed and such individuals and entities have executed a non-disclosure agreement. This independent deliberative process should be well-documented.

D. Transparency – Publication Rights

AMCs and collaborators such as large tech companies and digital health entrepreneurs will face the tension that typically exists between the collaborator's aversion to transparency so as to protect its IP and the associated competitive and commercial advantage and the AMC's desire to publish the findings on a current basis and thereby contribute to the rapid dissemination of generalizable knowledge to further biomedical innovation and improve health care delivery, research and medical education.

E. Tax-Exemption and Conflict of Interest Compliance Management

1. AI and other innovation investments (whether through an internal or third party investment fund, an entity created to commercialize home-grown technology, or a direct investment in a portfolio company of a third party fund), often involve the institution itself, the inventor of the discovery to be commercialized, other key clinical/scientific leaders, as well as members of the board and executive leadership teams. This is particularly true when the discovery to be commercialized is "home grown" – that is created by an institution's own clinicians and scientists either on their own or in connection with the roles and responsibilities they have within the institution.

a. On the one hand, investment and other involvement by key internal constituencies can generate the meaningful and effective support needed for a commercialization initiative that will successfully deliver the benefits of the invention to patients and the community at large.

b. On the other hand, complex, multi-dimensional conflicts of interests can arise from the fact that some or all of the individual and institutional investors may also play an active role in the selection of the venture in which to invest; the nature and extent of the investment; the leadership, governance and management of the venture entity; the further research and development undertaken by the venture to support commercialization; and, ultimately the purchase of the commercialized product marketed and sold by the venture entity.

2. Tax-Exemption and Conflict of interest and tax-exemption risks are closely interrelated and must be carefully and thoroughly assessed and managed to assure that the financial, research and clinical care decisions made with respect to the development, investment in and ultimate sales of commercialized AI products/services further the institution and its exempt mission and purposes in a manner that is consistent with the best interests, safety and health and welfare of the patients and communities the institution services and not the private interests of any individuals involved in in the commercialization effort.

a. Tax-Exemption

(i) Exempt Purpose and Unrelated Business Income.

A tax-exempt organization should internally address whether and how participation in AI or other technology innovation collaboration or investment transaction, including its provision of services and other support for the collaboration or commercialization vehicle, is substantially related to its 501(c)(3) purposes (promotion of health, research and education), particularly when one or more of the collaborators are private parties or taxable entities.

(a) Merely because an activity ultimately improves/promotes health or produces a stream of income for the AMC to use in furtherance of its exempt purposes does not make the activity substantially related. A key consideration is the extent to

which research results and other aspects of the development and outcomes of the collaboration/commercialization are available for publication by the tax-exempt organization and accessible at no charge by others. The terms and language of the collaboration agreement need to be consistent with the relatedness position. Self-serving language in the agreement and associated documentation is not sufficient

(b) Royalties and equity distributions may qualify for exclusion from unrelated taxable income but may still need to be incorporated into quantification of the AMC's overall unrelated business activity.

(ii) Private Inurement, Private Benefit and Intermediate Sanctions

(a) If officers, board/board committee members, other key personnel such as clinical or scientific leaders are investors in or otherwise financially interested in the outcome of the collaboration or investment and its outcomes, the tax-exempt organization's participation should be thoroughly reviewed and approved in accordance with the criteria for qualifying for the rebuttable presumption of reasonableness protection from intermediate sanctions under Section 4958 of the Internal Revenue Code, including review by a "disinterested" body with board-delegated authority, consideration of appropriate comparability data, and timely documentation of the review, deliberation and approval by the committee. The AMC would be well served to maintain a mechanism for and documentation of oversight of the collaboration by that same disinterested body.

(b) A tax-exempt organization's license fees/royalties, equity shares of an investment vehicle, payments for in-kind services, etc. must be fair market value/commercially reasonable and proportionate to its contributions, in cash and in kind (including technology licenses, tradename licenses, licenses to algorithms and tools, contribution of data, intellectual property assets, clinical expertise, administrative services, space, etc.).

(c) Valuation of the IP Rights and Negotiation of License Terms

(1) An independent valuation of the organization's relative contributions by a qualified expert is preferred be needed particularly if "insiders" or "disqualified persons" are also financially interested in the collaboration (e.g., co investors). However, if no insiders, Disqualified Persons or referral sources are involved as co-investors, an internal valuation that is well-reasoned, well-documented and performed before any equity share or other financial terms are proposed should suffice.

(2) An "after-the-fact" valuation will carry no credibility.

(d) Rebuttable Presumption Protection against Intermediate Sanctions

The Code Section 4958 Intermediate Sanctions Safe Harbor known as the "Rebuttable Presumption" should be scrupulously followed if the Creator or the Captive Investment Entity is engaging in an investment transaction with a "Disqualified Person" in accordance with the regulations under Section 4958. However, following the independent, thorough and well-documents process set forth in the criteria for qualifying for the rebuttable presumption is prudent for any co-investments with board/board committee members, management, or key clinical and research leaders of the investing organization and the investment entity. The independent review process discussed above with regard to

assessment of conflicts and overall oversight of the selection and implementation of investments will also contribute to achieving tax-exemption compliance including qualifying for the rebuttable presumption safe harbor.

(e) Tax-Exempt Financing Considerations

As noted above, a key up-front due diligence consideration is whether any of the space or facilities being provided for use by the collaboration/investment entity were financed with tax –exempt bonds subject to extremely tight allowance of "private use" and if so whether the proposed use and terms of the corresponding agreements would qualify for any current safe harbor protections.

b. Conflicts of Interest Compliance

Comprehensive, integrated conflicts of interest compliance oversight is essential throughout the life cycle of any collaboration or investment formed to develop and commercialize AI or other technology innovations.

(i) The decisions throughout the life cycle of the arrangement must be made by individuals who do not have conflicts of interest that can impair the integrity of the decisions so as to:

(a) avoid use of available resources primarily to further the financial interests of any individuals of entities (e.g., board members, senior management, key clinical and research leaders of Creator/Captive Investment Entity their family members or entities in which they have a material financial interest) rather than the purposes of the Creator and the Captive Investment Entity;

(b) protect against bias in clinical trials that can threaten the safety of human subjects participating in the trials and the integrity of the research data generated in support of approval for the commercialization and marketing of the product;

(c) prevent bias that leads to inappropriate purchasing of products and services of products manufactured by a spin-off or portfolio company in which the Captive Investment Entity invests for use in delivering clinical care; and

(d) prevent bias in the content of medical educational programs and materials in favor of products manufactured by an investor in a Venture or by a Venture itself.

(ii) If potential conflicts are appropriately identified and assessed at the very earliest stages of the innovation commercialization investment planning, conflict of interests should not become major roadblocks; if they are not, however, they can undermine the integrity of the initiative, cause major delays, or bring the effort to a screeching halt after substantial investments of time and money have been made.

(iii) Failure to address conflicts of interest in a thorough and timely way creates exposure to various compliance, liability and financial risks, including breach of fiduciary duty, violation of tax-exemption requirements, the inability to get or the loss of FDA marketing clearance, debarment from conducting federally-funded research, reputational damage and loss of public trust.

(iv) Maintaining integrity of decision-making in all important respects will require: (a) adoption and disciplined implementation of a conflicts of interest program for an

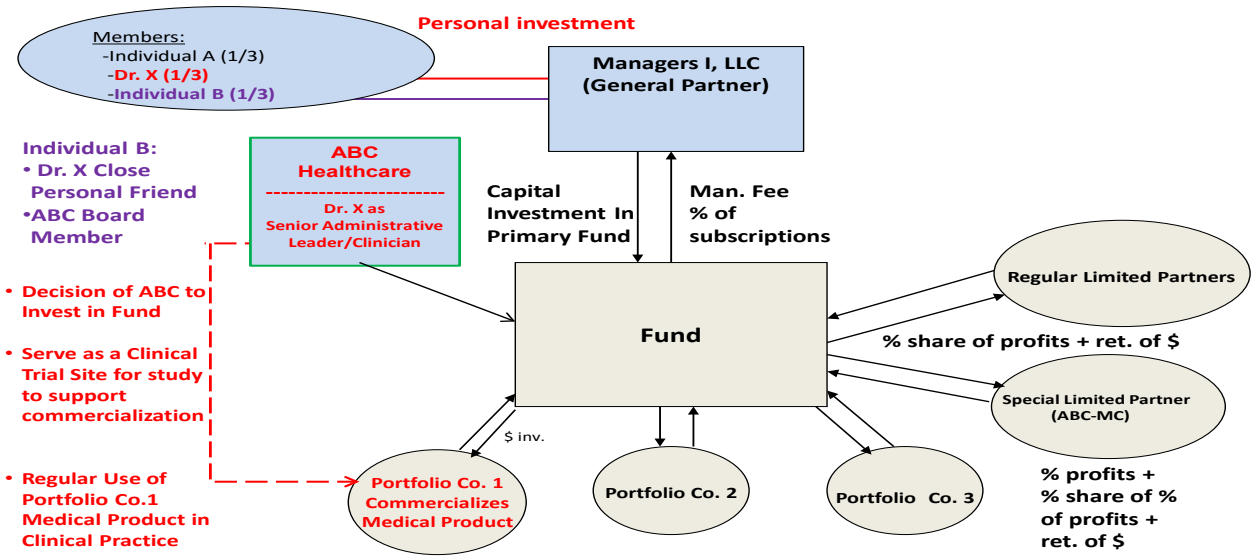
investment fund and spin-off; (b compliance with an organization's own conflicts of interest program; and (c careful integration of the two programs' compliance oversight of decisions made regard to initial and ongoing funding, and ongoing operation of, the collaboration and the investment vehicle.

(v) To manage potential conflicts of interest arising from any IP license or transfer arrangement, the technology transfer office involved in the IP licensing should handle valuation of the IP and negotiation of corresponding terms of the license or ownership transfer and should be "firewalled" from valuation and funding decisions the investment funding entity and its board will make with regard to the investing in the commercialization investment opportunity to which the IP license arrangement relates and if so under what structure and to what extent. Conflicts of Interest

(vi) The nature and extent of overlap between and among donors, board members, executives, key clinical and research leaders, and investors of an organization and the collaboration/investment vehicle will have a direct impact on establishing, assessing and maintaining the independence of those making key decisions for both organizations throughout the collaboration/life cycle, including: (a) decisions to provide initial and ongoing funding; (b) selection of board/committee, management and researchers; (c) contracting to provide administrative and other support; (d) becoming involved as a site and/or providing a principal investigator for a study conducted to support commercialization of the AI technology; and (e) purchasing a portfolio company's AI product/solution once commercialized.

(vii) The potential conflicts may be varied, including governance/management conflicts, research conflicts and clinical care conflicts, and the nature and extent of them may vary over the life of the development and implementation life cycle. Therefore, it may be necessary to revisit the conflicts assessment and management review periodically throughout the life of the collaboration. Again, the AMC would be well served by having that role performed by the disinterested body responsible for initial review and approval or the AMC's participation in the collaboration.

As illustrated by the **Diagram** below, establishing, assessing and maintaining independence will be particularly critical but challenging when various board/board committee members, management, inventors, and researchers, as well as the health care system itself, have a financial or associational interest that can be affected by commercialization investment decisions.



An organization's Board of Directors has ultimate responsibility for all dimensions of conflicts of interest compliance. The Board may fulfill that responsibility either directly or indirectly through the appointment of a committee. Which committee the Board uses will depend on the organization's overall governance structure and its committee structure in particular. In all cases, clearly delineating and documenting the lines of responsibility and accountability for conflicts of interest compliance is essential and individuals performing the conflicts role must be individuals who both have no conflicts of interest relating to a proposed venture investment and have appropriate qualifications and are fully independent.

F. Fraud and Abuse

Co-investment or other collaborations with individuals or entities in a position to refer to or order from a provider products and services reimbursed under Medicare generally or considered "Designated Health Services" under the federal Stark Law, and other financial involvement of such individuals (e.g., clinical/research consulting agreements, research agreements, shares of royalty income under license arrangements) must be carefully structure to avoid violations of the Medicare anti-kickback prohibition and the Stark self-referral prohibition. Following are some fundamental guideposts for structuring the investment interests, implementing the investment transaction, and operating the commercialization venture.

1. Investment entities must be "real" companies with real assets, liabilities and operations. While the provider-investor may provide some funding and in-kind support, neither should be the majority of the financial and other resources needed to support the entities' operations or those of any spinoff/portfolio company. The provider-investor and the investment entity must be reimbursed for any costs they incur beyond those.

2. The provider-investor cannot act as a "free incubator" that transfers businesses once they are "on their feet" to the Captive for co-investment with referral sources without compensation. In that regard, the Creator can fund the costs of the early development and formation of the Captive Investment Entity and the Captive Investment Entity can do the same with regard to spinoffs/portfolio companies. However, referral sources must pay directly the costs they incur in connection with their own assessment and implementation of their investment in the commercialization entity.

3. The provider-investor and investors/investment entities all must receive compensation that is commercially reasonable and fair market value for their services and other support as well as space, equipment and supplies they provide to the endeavor.

4. The individuals who split their time between responsibilities to the provider-investor and investment entity and the support they are providing to the investment entity and any spinoff/portfolio companies must regularly track and document the time they spend and any costs they incur in their roles for each entity and the agreements for the provision of such support should clearly delineate the applicable responsibilities and time.

5. Compensation if any paid to referral sources for service on the boards of investment entity and any spinoff/portfolio company must be consistent with the compensation paid to all board members.

6. Allocation of investment opportunities should not involve "cherry picking" of investments in which referral sources will be co-investors as a means of providing them with indirect financial benefits.

G. Common Rule and HIPAA Regulation of Human Subject Research

Whether the research and development efforts undertaken at any stage of the commercialization effort constitute human subject research regulated by the Common Rule, HIPAA and the FDA research regulations is an essential, threshold consideration and if so what consents, authorizations or other pathways must be followed in order to comply with the applicable requirements of those laws.

H. FDA Pre-Market Approval Requirements

Whether the invention to be commercialized is regulated by the FDA is another essential, threshold consideration and if so under which of the FDA's product classification system. If so, the spinoff/portfolio company will need the policies, procedures, and resources needed to meet the FDA pre-market research, quality and application requirements that apply to the product classification.

VI. Integrating Technology Innovation Compliance Oversight and Management into Current Compliance Program Content and Operations

The following is a discussion of high level recommendations for consideration in building on the strength of an existing compliance program content and operations to integrate Innovation compliance risk management dimensions into the compliance program in a way that enhances the effectiveness of both the program and the Innovation domain under the umbrella of enterprise risk management. These recommendations are not intended to be exhaustive or to prescribe the approach for implementing them. There will be various avenues for implementing them. Some may require new policies, others may merely require changes to existing policies, while others may be addressed by existing compliance program elements such as monitoring and training..

A. Innovation-Related Compliance Risk Areas And Proposed Enhancements

The following is a discussion of key compliance risk areas it will be important for the compliance program content and operations to address for purposes of managing the risk of digital health technology innovation including AI-powered solutions. Addressing these risk areas in policies and procedures may require addition of some existing policies and addition of new policies. The approach used should be carefully tailored to the structure and content of the current program.

1. *Billing and Coding Compliance for Delivery of Innovative Care Solutions*. Billing and coding requirements and practices applicable to AI-powered and other care delivery innovations are complex, unclear, non-harmonized, and constantly changing. They are rapidly evolving and are the focus of increasing scrutiny by commercial and government payers due to high error rates.[231] A compliance program should be adapted to include policies, procedures and ongoing monitoring that addresses address this somewhat novel and unsettled dimension of compliance

2. *Compliance with Quality and Safety Standards Related to Innovation Solutions in Care Delivery*. Innovation solutions by their nature typically require an approach to quality and safety standards that differs from those developed for more traditional care delivery methods. The standards will be important for managing the new dimensions of quality and safety liability risk presented by new delivery modes, particularly virtual ones. Such standards would logically be designed and implemented primarily by the quality and safety risk oversight group as part of its role within the overall enterprise risk management ("ERM") initiative, but the failure to comply with quality and safety standards can lead to legal and regulatory compliance risk.[232] The following are two relevant bodies of standards below that we recommend the Program address.

3. *Compliance with State Professional Practice Standards*. The delivery of care using Innovation solutions is often regulated both directly and indirectly by the states' licensure and registration laws and professional standard setting and oversight bodies in ways that create Innovation implementation hurdles (and at times barriers) that are also novel, non-harmonized, ever-evolving and, as a result, frequently overlooked. Identifying and assessing applicable state(s) clinical practice statutes and regulations, including scope of healthcare professional practice restrictions, prescribing restrictions and pharmacy laws, corporate practice of medicine restrictions, healthcare consumer protection laws and regulations, informed consent and other requirements, prior to delivering care using a new Innovation solution or in an expanded geography, will be essential. Therefore, corresponding changes to compliance program policies addressing such interrelated compliance risks may be needed to maintain alignment of the compliance program with such other standards and effective management of quality and safety-related compliance risk.

4. *Compliance with The Joint Commission Standards*. The Joint Commission Accreditation Standards for Hospitals and Health Systems pertaining to telehealth require hospitals to follow specific processes and standards.

5. *Compliance with FDA Regulations on Pre-Market Approval of Medical Devices*. Whether and to what extent digital health and other healthcare technology Innovations are subject to Food & Drug Administration ("FDA") pre-market approval requirements for medical devices has been a particularly challenging compliance issue over the past few years. The applicable

[231] See, for example, the recent OIG Workplan focus on billing errors in innovative telehealth technologies in the OIG Workplan for 2018-19. https://www.beckershospitalreview.com/healthcare-information-technology/managing-fraud-waste-and-abuse-during-the-expansion-of-telehealth.html

[232] One example in the Innovation context includes instances of potential malpractice or other bad outcomes that could flag the need to conduct a compliance review of whether the corresponding services should have been billed, or if not yet billed whether they should be, in order to assess the need to make a repayment/self-disclosure for claims that were filed or the need to hold the filing of claims that have not yet been filed pending the outcome of the review. Another is instances in which peer review/credentialing findings indicate care was provided by personnel with less than legally-required qualifications and flag the need to consider conducting a compliance review of whether the services should have been billed, or if not yet billed whether they should be, in order to assess the need to make a repayment/self-disclosure for claims that were filed or the need to hold the filing of claims that have not yet been filed pending the outcome of the review.

law provides a basis for the FDA to cast a broad jurisdictional net over Innovation solutions. The focus of the pre-market approval requirements is on the safety and effectiveness of Innovation products and solutions both on a stand-alone basis and when connected with or companion to another product or solution. The FDA is also increasingly concerned about safety issues arising from potential for hacking of life-sustaining and other health care devices. Although the FDA has been endeavoring to adopt new regulations and enforcement positions that will help to accelerate health care Innovation, it has also been enforcing applicable law as it currently stands. Non-compliance by third party entities in which an organization invests directly or indirectly through funds may indirectly expose the organization to government or media scrutiny and associated reputational risk. Such non-compliance can also result in denial of FDA approval or post-approval warning letters or enforcement initiatives that delay or totally disrupt the marketing and sale of the solution and associated loss on the investment.

6. *Compliance with FDA and FTC Regulation of Marketing and Promotion of AI Solutions*. Accurately portraying the functionality and benefits of both home-grown and externally developed AI innovations is essential to avoid inadvertent violations of legal and regulatory requirements and prohibitions such as FDA requirements for labeling, advertising and promotion of medical device, FTC consumer fraud and misrepresentation prohibitions; and myriad state consumer protection laws. Incorporating into a compliance program content standards, marketing and promotion "do's and don'ts" and requirements and procedures for review of marketing and promotional materials throughout the life cycle of Innovation solutions will contribute significantly to the management of these risks. The key focus of such content requirements and review would be whether the marketing and promotional materials accurately describe the nature of the solution and its intended results for patients and consumers. Accurately portraying a health care system's role is also important for liability and reputation risk management. A separate but important legal consideration is protection of its name, trademarks, and other intellectual property in the solutions.

7. *Clinical Reliance upon Consumer Generated Data*. Physicians regularly receive requests from patients to review and receive data gathered from consumer wellness devices (*e.g.*, EKG data from an Apple Watch). Moreover, collection and use of consumer generated data is integral and prevalent in AI-powered patient and consumer-facing digital health solutions. Key compliance considerations include, among others, privacy and security by design standards and patient consent practices that meet emerging legal requirements and standards for electronic communications empowered by mobile devices and the Internet of Things.

8. *Secondary Use of Patient and Consumer Data*.

a. Collection, aggregation and analysis of data of various types and from various sources is an essential ingredient in both the development and implementation of most if not all forms of Innovation. Robust repositories of such data are also now viewed as valuable assets that are being leveraged in various ways in the context of Innovations investments and commercialization initiatives. Whether and how to leverage the value of such data repositories presents both significant opportunities and significant compliance, reputation and patient trust risks and consequences that need to be carefully identified, assessed and managed in a cohesive and integrated way on an enterprise-wide basis.

b. Adopting over-arching principles and supporting guidelines and criteria for determining whether, when and how patient and consumer data should be leveraged in support of AI and other Innovation opportunities, coupled with appropriate governance and management oversight, is essential to avoid undue or inadvertent non-compliance and associated scrutiny and objections by the government, the media, patients and the public at large. Such principles, guidelines and criteria should be developed and approved at the

highest levels of senior or executive management and approved by the board or an appropriate board committee.

9. *Communicating with the Government on Use and Offering of Innovation Solutions*. As an organization delves deeper into innovation, it may encounter the need on a more regular basis to consult with government regulators (*e.g.*, state regulatory boards, FDA inspections, and government payors) concerning innovation compliance dimension and enforcement positions that are unclear and in a state of flux. Guidelines for whether, when, how and by whom such outreach to governmental authorities should be undertaken will support good faith compliance efforts and help to avoid undue or inadvertent non-compliance and unnecessary government scrutiny.

VII. Effective Oversight of AI and other Technology Innovation Initiatives – Maximizing Resources and Opportunities While Managing Compliance and other Enterprise Risks

A. The Need for a Comprehensive, Integrated and Multi-Disciplinary Approach to AI Innovation Oversight

1. With the recent explosion in digital health, the opportunities for digital health innovation seem to abound and are likely to arise in various corners of an organization's day-to-day world, including one or more clinical departments, strategic business development, IT, tech transfer, sponsored research, to name a few. In many instances, those spearheading the initiative are not aware of the complexities and the complications and waste of valuable resources that can result from planning and development approaches that do not look at the opportunity from a comprehensive, strategic and enterprise risk perspective. Adoption of a simple telemedicine program to expand behavioral health capabilities, for example, may utilize systems that are incompatible with the existing IT platform and make the protection of highly sensitive information more complicated. Worse, a seemingly simple digital health solution could result in nuanced compliance risk not recognized by the adopter. And, from a financial perspective, substantial resources may be devoted to an initiative that does not serve one of the key strategic priorities of the system and diminish resources that are then available for initiatives that would. In short, multiple digital health initiatives running in multiple locations within a system without proper vetting and oversight can create dramatic inefficiencies, wasting of valuable resources and lost strategic opportunities.

2. A centralized, multi-disciplinary Technology Innovation Governance Program structure governance program that centralizes important can play a key role in avoids these risks, particularly for large, sophisticated AMCs and integrated delivery systems. "Digital Health Governance" is not "Data Governance" under a new name and, while the two regimes relate to one another, they should not be considered interchangeable. Technology Innovation Governance has a much broader scope than Data Governance - it is an integrated approach that oversees digital health innovation from a comprehensive enterprise risk perspective, and as such should include representatives from legal, compliance, finance, clinical care generally, quality and patient safety, risk management, technology and strategy/business development.

3. Technology Innovation Governance may come with some growing pains for an organization as it necessarily brings into closer coordination departments that may have historically operated somewhat independently from one another, perhaps even by design. Therefore, a thoughtful roll-out and implementation process is key. A few key elements for a successful roll out include:

a. Selection of the right business "lead" or "owner" of both the roll-out and the implementation.

b. Clear and concise charter, policies and procedures that take into account the complimentary responsibilities of existing business and compliance committees and departments.

c. Education of team, senior leadership and the board.

d. Thorough and system-wide education, together with the setting of clear expectations regarding cooperation and collaboration.

e. Recognition that evolution of the structure may be appropriate over time.

4. There is no one size fits all approach or structure.

a. The right structure will take into account the size, complexity and strategic plan of the entity, as well as its own particular culture.

b. A phased approached may be most appropriate and effective. For example, starting with just a single leader and then move to a more robust management oversight coupled with formal delegation for board oversight to the appropriate committee.

c. Under the single leader, robust committee or any other approach, official selection and delegation of authority and responsibility for leading the Technology Innovation Governance initiative will be essential. Whomever is chosen should not only have the necessary legal skills but also good project management and communication skills.

d. Like a compliance program infrastructure, the approach should be designed with what will achieve the most effective oversight and risk management based on the particular culture, compliance and enterprise risk programs, and over management and governance structure of the organization.

B. Possible Structures – Conceptual Descriptions

Following are below possible approaches we have seen used, one or a combination of which may be worthwhile.

1. Single leader supported by ad hoc staff.

For an organization that may have fewer Technology Innovation Governance demands and a need to pull together different stakeholders for different assessment but only as needed, a single leader with ad hoc staff and support may be the right scale. The advantages with this approach may include: (a) stronger sense of responsibility and create clear path of accountability, (b) streamlined process can result in rapid decision making, and (c) departments remain unburdened by additional "committee" assignments. The disadvantages with this approach may include: (a) potential for lack of interest / development of expertise within different operating divisions, (b) increased likelihood of an issue being missed by a single coordinator, and (c) lost opportunity for cross-learning among departments.

2. Management Oversight Committee

For an organization whose size, internal politics, and/or complexity suggest that digital health evaluation and implementation issues will be under consideration on a regular basis and will touch on the portfolio of diverse stakeholders, a standing committee may be best. The advantages with this approach may include: (a) increased likelihood that cross-department

collaboration and learning will improve digital health literacy across the organization, (b) comprehensive "issue spotting" and "issue resolution" will occur with every opportunity under consideration, and (c) increased cross-departmental awareness of organizational needs. The disadvantages with this approach may include: (a) potential for slower decision-making and difficulty getting to "yes", (b) potential for diminished commitment if committee structure proves slow or burdensome, and (c) shared responsibility may reduce sense of individual responsibility.

3. Board Subcommittee Oversight

For organizations not ready to commit to actively managing digital health opportunities from a system perspective, or wishing to exercise more significant board oversight of digital health opportunities and initiatives, a board subcommittee may be appropriate. The advantages with this approach may include: (a) ensuring appropriate board-level attention and focus, and (b) board-level education regarding digital health matters becomes easier. The disadvantages with this approach may include: (a) without an operating or management structure in support, the board subcommittee may have incomplete or imperfect information, and (b) without active management by a dedicated team, subcommittee directives may not be as effectively carried out.

C. Representative Real World Example

See Attachment F for an illustration of one possible approach for establishing a formal, well-defined, and centralized structure and process for a streamlined review and approval of technology innovation opportunities that takes strategy-driven and integrated approach to overall enterprise risk assessment and management, including, among others, compliance, financial, and strategic risks. This approach is intended to: (1) establish a single entry point for intake and assessment of proposed innovation initiatives according to intake and assessment criteria, guidelines and policies; (2) clearly identify where decision-making authority with regard to technology innovation initiatives resides; (3) utilize clear and empowering delegation criteria to assign to the appropriate decision-making bodies the responsibility and authority to conduct initial intake and assessment and to recommend, and give final approval for, implementation of an appropriate range of technology innovation initiatives; (4) facilitate timely and responsive guidance on the strategic, programmatic, financial, compliance, legal, technical, and other key risk dimensions; and (5) support ongoing monitoring of compliance and other enterprise risks associated with Innovation initiatives.[233]

D. Effective Data Governance Program

1. Background

a. "Data Governance," has emerged largely from the Big Data and Digital Health revolution both to create and leverage the value of data and to manage the associated dimensions of enterprise risk. Data governance is particularly important with respect to AI-powered innovation initiatives because of the "black box" dimension of AI and its significant dependence on vast quantities of data from various sources in the data ecosystem.

b. Data Governance is viewed as an "organizational responsibility" and as such should emanate from and be included within the overall oversight responsibility of the Board of Directors. Leading commentators have expressed the view that "[R]igorous controls on how data are used and by whom, careful and considered alignment of interests, and

[233] E.g., the Brigham and Women's Hospital model is recognized for accomplishing these objectives: https://www.bwhihub.org/about/

focused investments in long-term capability-building are important starting points for this new and expanding frontier of collaboration."

c. Harvey Krumholz, professor of medicine and public health at Yale University and a member of PCORI's board of governors, observed that the quality of the data exchanged over time through data collaborations will improve over time through both experience in using the data and the development of more complete data governance plans.[234]

d. What constitutes an effective Data Governance program is evolving; both today and in the future, it will likely vary both across and within an industry. No common, industry-standard or best practice approach has emerged. Following is a summary of some of the principles, guidelines and approaches that have been developed and used to date (and is not intended as comprehensive or all-inclusive).

2. Scope and Approach

An effective Data Governance program, which would work hand in hand with the enterprise-wide Technology Innovation Governance program discussed: (a) takes an integrated, enterprise-wide approach that encompasses all operational domains (e.g., financial/administrative, IT, clinical, research, education) within the enterprise, with domain-specific governance policies and procedures that are consistent with a common governance framework; and (b) proactively strives to stop data-related problems before they begin by reducing ambiguity, establishing clear accountabilities, and disseminating data-related information to all stakeholders.

3. Key Components

A data governance framework should include the following common core components:

a. Principles – articulation of the high level objectives of the data governance program;

b. Organization – establishment of an organizational structure that (a) encompasses roles, responsibilities, decision-making authority and accountability for meeting objectives, resolving disputes, and aligning stakeholders across the enterprise, and (b) strong executive leadership and commitment from clinical, business and IT stakeholders;

c. Standards and Processes – to promote common terminology and data definitions, including quantitative metrics for data quality, with process and workflows for each data domain within the organization; and

d. Technology – tools to support the definition, application and compliance measurement of data governance policies, standards and processes across the enterprise.

4. Key Focus Areas

Key focus areas of the data governance framework include the following: (i) data definitions; (ii) data quality/integrity (e.g., accuracy, completeness/gaps, timeliness, consistency, semantics); (iii) data availability (e.g., uninterrupted access, disaster recovery plan); (iv) data architecture; (v) data Integration; (vi) data ownership; (vii) data sensitivity; (viii) compliance risk (e.g., privacy and security, antitrust); (ix) strategic and financial risk; (x) data storage and retention (e.g., metadata management, internal v. external storage); (xi) leveraging of data;

[234] 65 Fed. Reg. 82,462, 82,608 (Dec. 28, 2000).

and (xii) relationships with third parties (e.g., who gets your data, from whom do you get data, who can access and use your data).

5. Data-Driven Collaborations with Third Parties

An important component of a Data Governance Program would be the development of **principles, criteria and guidelines** for evaluating whether to license or otherwise make either or both identifiable or de-identified patient information available to a third party to support an AI-focused collaboration and for unrelated secondary uses by the collaborator and for implementing such arrangement within acceptable compliance parameters.

a. Of course, a core focus of any set of data governance principles and criteria would be compliance with federal, state and international laws protecting the privacy and security of individual health-related and other personal data.

b. For health systems and other providers, however, a fundamental threshold consideration is the risk that providing patient data (whether identifiable or non-identifiable), even under permissible compliance pathways will threaten public trust and confidence as well as reputation - two priceless assets.

c. Following is an example of key factors/variables to be taken into account in the development of principles, criteria and guidelines to support identification and assessment of compliance, patient relations and reputational risks:

(i) Nature of the entity to which the data will be provided?

(a) Nonprofit/Tax-Exempt (e.g., trade association, professional society registry, government agencies, community service organizations, Accountable Care Organizations)

(b) Proprietary (e.g., IT vendors and other business associates, pharma/biomed, clinical/molecular testing laboratories, pharmaceutical companies, medical device companies, eCommerce companies (e.g., Google, Amazon), inventors/entrepreneurs)

(ii) Nexus between proposed use of the data and the mission/purpose of the organization providing the data. For example:

(a) Close Nexus: use for tumor boards, grand rounds, disease registries, quality improvement, care management and coordination, population health management, accreditation/evaluation of providers, training, public health surveillance and improvement, IRB-approved human subject research using retrospective data analysis

(b) Moderate Nexus: use in support of a collaboration between the health system or other covered entity and a third party to develop an AI solution that will enhance the delivery of care or other dimension of the covered entity's mission, or

(c) No Nexus: use by the third party recipient for its own business purposes and to generate a profit (e.g., testing and enhancement of existing products/services, new product development, development/enhancement of a robust data repository of data for licensing to pharma/device companies and other third parties)

As a general rule, the closer the alignment of the primary and secondary use of the data is with the covered entity's health care deliver, research and education missions the lower will be the actual or potential risk.

(iii) Data being contributed/exchanged

(a) Will the data come in various non-standardized forms? Structured or Unstructured?

(b) Will it be combined with data in various forms and from various sources (e.g., consumer-generated data, literature; structured or unstructured)?

(c) Will it contain types of information subject to special protections under laws other than HIPAA/HITECH (e.g., state law, GINA, COPAA, state laws)?

(d) Will any competitively sensitive information of competitors be involved?

(e) What was the original purpose for which data was contributed/exchanged?

(f) Will it contain "identifying" information when contributed?

(g) Will it contain "identifying" information when used/accessed by recipient?

(h) Was there a consent, authorization or other pathway for the proposed used put in place at the time the data was initially created/received?

(i) Will the data be de-identified, or a limited data set derived from it, prior to using the data for secondary purposes? If so, who will do the de-identification and what de-identification standard will be required?

(iv) Will the entity contributing the data receive any remuneration from the data recipient or other collaborators? If so, in what form (cost reimbursement, royalty, equity, service fees), and how does the amount compare to the cost incurred to contribute information to the arrangement?

(v) Will the data will be stored and/or used on a cloud? Who provides the cloud – the data recipient or a third party vendor? Where are the servers and the personnel supporting them – U.S. or Off Shore? Will the cloud be a multi-tenant cloud or a shared cloud with appropriate segregation?

ATTACHMENT A

Glossary of Other Relevant Terms

1. "Application Programming Interface" or "API"

Like a power outlet that relies on a common set of electronic principles to enable different electronic devices to use the power outlet from various locations to "plug in" to the power grid and receive the electricity needed to power the device, an Application Programming Interface consists of a common set of programming principles that allows websites and mobile applications to "plug in" and receive computable information.

2. "**Clinical Decision Support Software**" (**CDS Software**) is technology that "provides health care providers and patients with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care."[235] While it might enhance, inform, or influence health care decisions, it is not intended to replace a clinician's judgment. Examples include software that provides access to: (a) computerized alerts/reminders for providers and patients; (b) contextually-relevant reference information (e.g., clinical guidelines); (c) condition-specific order sets; (d) focused patient data reports and summaries; (e) documentation templates; (f) diagnostic support; and (g) recommendations for patient management.[236]

3. "Cloud Computing"

Cloud computing has become integral to any complex data sharing and analytics strategy. By its very nature, it involves one or more third party support organizations. Particularly with regard to data center/server capacity and disaster recovery plans, a prime vendor often has relationships with various subcontractors, and such subcontractors from time to time are located "off shore."

(a) Five Essential Characteristics

(1) Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet and which will play an essential role in any digital health solution.

(2) Regardless of service or deployment model, there are five essential characteristics of cloud computing:

(i) on-demand self-service offerings that enable users to access cloud-based services at their convenience, without having to interact directly with the service provider;

(ii) broad network access, effectively allowing users to access cloud-based services from any internet-enabled device;

---

[235] U.S. FOOD AND DRUG ADMINISTRATION (FDA), FEDERAL COMMUNICATIONS COMMISSION (FCC), & OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY (ONC), *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* (2014), *available at* http://www.healthit.gov/sites/default/iles/fdasiahealthitreport_final.pdf (last visited June 14, 2016).

[236] Michael W. Ryan, *Work in Progress: FDA's Regulation of Health Information Technology*, FOOD AND DRUG LAW INSTITUTE 16 UPDATE JULY/AUGUST 2014, (July/August 2014), *available at* https://www.mwe.com/~/media/files/thought-leadership/publications/2014/07/work-in-progress-fdas-regulation-of-health-infor__/files/unnamed-item/fileattachment/fdli_ryan_julyaug2014.pdf

(iii) availability of pooled resources so that multiple consumers can be served, "with different physical and virtual resources dynamically assigned and reassigned according to consumer demand";237

(iv) flexibility with respect to system capabilities, which may be "rapidly and elastically provisioned to quickly scale out, and rapidly released to scale in";238 and

(v) control and optimization of resources by "leveraging a metering capability at some level of abstraction appropriate to the type of service."239

(b) Three Service Models

While some overlap exists among the three principal cloud computing service models, each model possesses distinguishing characteristics relating to the services offered and varying levels of control of the parties over the technology involved.

(1) Software as a Service (SaaS)

SaaS currently occupies, and is expected to continue to occupy – a majority of the global public cloud market. [240] With the SaaS model, consumers access the cloud provider's software applications from various client devices through a thin client interface such as a web browser. While the computing, processing and storage capabilities of the application are perceived by consumers to exist "in the cloud," these processes actually take place in the cloud provider's data center. The user does not manage or control the underlying cloud infrastructure.[241] Examples include Google's Gmail and Google Docs.

(2) Platform as a Service (PaaS)

The PaaS model allows consumers to use the cloud network to create, deliver and deploy software applications on the cloud infrastructure. As with the SaaS model, PaaS users do not control the underlying cloud infrastructure. However, in contrast with the SaaS model, PaaS users maintain a significant level of control over the applications that are deployed into the cloud.

While SaaS applications are routinely used by even the most novice consumers, PaaS services generally appeal to individuals with technical expertise. The PaaS consumer-base is likely to include application developers, administrators, testers and deployers.[242] Once a PaaS consumer deploys an application into the cloud, that application will be perceived by end-users – and rightly so – as a SaaS application. Thus, PaaS services can function as a step in the process of developing and deploying SaaS applications. Examples include Google Apps, Force.com.

(3) Infrastructure as a Service (IaaS)

The IaaS model provides consumers with access to additional computing resources, such as processing, storage and other fundamental computing resources on an as-needed basis.[243] In

---

[237] *Id.*
[238] *Id.*
[239] *Id.*
[240] Larry Dignan, *Cloud Computing Market: $241 Billion in 2020*, ZDNET (Apr. 22, 2011), http://www.zdnet.com/blog/btl/cloud-computing-market-241-billion-in-2020/47702 (last visited June 14, 2016).
[241] *Id.*
[242] *Id.*
[243] *Id.*

simplest terms, IaaS services function as an alternative to purchasing new hardware. The consumer does not have control over the underlying cloud infrastructure, but maintains control over operating systems, deployed applications, storage and some network features, such as firewalls. Examples include Rackspace, IBM, and Amazon Web Services.

(c) Four Models of Accessibility

Generally, there are four deployment models: (i) Private Clouds; (ii) Community Clouds; (iii) Public Clouds; and (iv) Hybrid Clouds. In large part, the appropriate deployment model depends on the relationship between the service provider and the end-user and among the end-users. The deployment model selected affects which users may access the cloud, who manages the cloud and where the cloud is located.[244]

4. "**EHR System**" is "… a real time patient-centered record that allows access to evidence-based tools that can aid providers in decision-making. The EHR can automate and streamline clinician's workflow, ensuring that all clinical information is communicated. It can also prevent delays in response that result in gaps in care. The EHR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting."[245]

5. "Health Information Technology" (Health IT) refers to a group of tools that promise to improve health outcomes and reduce health care costs by enabling the measurement, collection, storage, aggregation and transmission of patient-specific and publicly-available health information, analyzing data using publicly-available and proprietary algorithms, and making recommendations for patient diagnoses and patient management."246

6. "**Medical Device**" is any "instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article" that is "**intended for use** in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment or prevention of disease…" [Emphasis added.][247] "**Intended use**" means the **objective** intent of the persons legally responsible for labeling the device, which can be manifested by expressions or by the circumstances surrounding the distribution of the product (e.g., text of the label or instructions for use, press releases, statements by manufacturer representatives (in person, media coverage, presentations, social media), brochures).

7. Medical Device Data Systems (**MDDS**) are devices through which data are "passively transferred or communicated, without controlling or altering the functions or parameters of any connected medical device(s)," and that are intended for one or more of the following uses:

(a) The electronic transfer of medical device data (i.e., any electronic data that is available directly from a medical device or that was obtained originally from a medical device);

(b) The electronic storage of medical device data;

---

[244] *Id.*

[245] U.S. FOOD AND DRUG ADMINISTRATION (FDA), FEDERAL COMMUNICATIONS COMMISSION (FCC), & OFFICE OF THE NATIONAL COORDINATOR FOR HEALTH INFORMATION TECHNOLOGY (ONC), *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* (2014), *available at* https://www.healthit.gov/sites/default/files/fdasia_healthitreport_final.pdf.

[246] Michael W. Ryan, *Work in Progress: FDA's Regulation of Health Information Technology*, FOOD AND DRUG LAW INSTITUTE 16 UPDATE JULY/AUGUST 2014, (July/August 2014), *available at* https://www.mwe.com/~/media/files/thought-leadership/publications/2014/07/work-in-progress-fdas-regulation-of-health-infor__/files/unnamed-item/fileattachment/fdli_ryan_julyaug2014.pdf (last visited June 14, 2016).

[247] 21 U.S.C. § 321(h).

(c) The electronic conversion of medical device data from one format to another in accordance with a preset specification; or

(d) The electronic display of medical device data.[248]

Note: A MDDS is not a system that performs any other function and does not: (i) modify, interpret, or add value to medical device data (or the display of the data); (ii) create or generate any of its own data (except for information regarding the MDDS' functioning); (iii) Process, characterize, categorize or analyze medical device data; (iv) flag, prioritize, plot, or graph medical device data (if such uses would add value to the existing data); or (v) facilitate active patient monitoring.

[248] 21 CFR § 880.6319.

ATTACHMENT B

"PERFECT STORM" OF COMPLIANCE REQUIREMENTS AND ASSOCIATED ENTERPRISE RISKS

Keenly Interested Regulators/Other Watchdogs	Applicable Legal/Compliance Area	Examples of Potential Consequences of Non-Compliance***
Food and Drug Administration (FDA)	□ Pre-Market Approval of "Medical Devices" □ Safety of Subjects and Integrity of Data in Research Supporting Market Approval □ Truth/Transparency in Marketing/Advertising	□ Denial/Withdrawal of Marketing Approval □ Suspension/Termination of Research Study □ Monetary Sanctions/Penalties □ Criminal Penalties
Office for Human Research Protections (OHRP)	Protection of Safety of Human Subjects in Federally Funded Research	□ Debarment of institution and researchers from participation in federally-funded research □ Suspension of Civil and criminal penalties, incl. expulsion from research programs
Office for Civil Rights(OCR)	□ Privacy and Security of Patient Data □ Protection of Individual Rights	□ Privacy Violation Monetary Sanctions □ Data Breach Reporting, Notices and Monetary Sanctions
State Authorities with Privacy/Security Compliance Oversight (e.g. Attorneys General)	□ Constitutional Rights of Privacy □ State Statutory Personal/Medical/Sensitive Information Privacy and Confidentiality Protections □ State Consumer Protection Laws protecting Patient and Consumer Rights	Civil and criminal penalties
Federal Communications Commission	Communications Technologies and Consumer Protection	Civil penalties
Federal Trade Commission	Consumer Protection □ Unfair and Deceptive Trade Practices □ Truth in Advertising	Civil and potentially criminal penalties
State Consumer Protection Agencies	See directly above	Civil and potentially criminal penalties
□ State Corporate Practice of Medicine Prohibitions □ Professional Boards Practice Standards	□ Failure to Meet Professional Practice Standards and Associated Standard of Care □ Violation of Permitted Scope of Licensed Professional Practice □ Corporate Practice Restrictions	□ Suspension/Loss of License □ Injunctions □ Civil monetary penalties □ Potential criminal penalties □ Provider-initiated lawsuits against employer
Drug Enforcement Agency	Prescription and Distribution of Controlled Substances	Civil and potentially criminal penalties
State Departments of Insurance	□ Payor Coverage	Civil damages, fines and penalties
□ HHS Office of Inspector General (OIG) □ Department of Justice	□ Marketing Practices □ Financial Relationships with Referral Sources/Recipients □ Beneficiary Engagement and Incentives	□ Civil penalties □ Criminal sanctions
Centers for Medicare and Medicaid Services	Reimbursement for Innovative Products and Solutions	□ Civil penalties □ Criminal penalties □ Exclusion from federal programs
Securities and Exchange Commission	Management and Reporting of Investments in Digital Health Solutions, Investor Disclosures and Protections	□ Civil penalties □ Criminal penalties
The Joint Commission	Accreditation of Healthcare Providers using Digital Health Solutions	Loss or suspension of accreditation status
Class Action Bar	Safety of patients/research subjects/consumers □ Personal injury/harm □ Breach of privacy/confidentiality of personal information □ Violations of TCPA	□ Civil damages □ Fines/Injunctions under TCPA
Prominent Media Outlets	□ Any one or more of the above	□ Damage to Reputation □ Erosion of Patient/Consumer Trust

Attachment C

General Framework for Considering Clinical Artificial Intelligence Quality and Safety[249]

Table 1 A general framework for considering clinical artificial intelligence (AI) quality and safety issues in medicine

Issue	Summary	Example
Short term		
Distributional shift	A mismatch between the data or environment the system is trained on and that used in operation, due to bias in the training set, change over time, or use of the system in a different population, may result in an erroneous 'out of sample' prediction.	The accuracy of a system which predicts impending acute kidney injury based on other health records data, became less accurate over time as disease patterns changed.[40]
Insensitivity to impact	A system makes predictions that fail to take into account the impact of false positive or false negative predictions within the clinical context of use.	An unsafe diagnostic system is trained to be maximally accurate by correctly diagnosing benign lesions at the expense of occasionally missing malignancy.[6]
Black box decision making	A system's predictions are not open to inspection or interpretation and can only be judged as correct based on the final outcome.	A X-Ray analysis AI system could be inaccurate in certain scenarios because of a problem with training data, but as a black box this is not possible to predict and will only become apparent after prolonged use.[9]
Unsafe failure mode	A system produces a prediction when it has no confidence in the prediction accuracy, or when it has insufficient information to make the prediction.	An unsafe AI decision support system may predict a low risk of a disease when some relevant data is missing. Without any information about the prediction confidence, a clinician may not realise how untrustworthy this prediction is.[46]
Medium term		
Automation complacency	A system's predictions are given more weight than they deserve as the system is seen as infallible or confirming initial assumptions.	The busy clinician ceases to consider alternatives when a usually predictable AI system agrees with their diagnosis.[48]
Reinforcement of outmoded practice	A system is trained on historical data which reinforces existing practice, and cannot adapt to new developments or sudden changes in policy	A drug is withdrawn due to safety concerns but the AI decision support system cannot adapt as it has no historical data on the alternative.
Self-fulfilling prediction	Implementation of a system indirectly reinforces the outcome it is designed to detect.	A system trained on outcome data, predicts that certain cancer patients have a poor prognosis. This results in them having palliative rather than curative treatment, reinforcing the learnt behaviour.
Long term		
Negative side effects	System learns to perform a narrow function that fails to take account of some wider context creating a dangerous unintended consequence.	An autonomous ventilator derives a ventilation strategy that successfully maintains short term oxygenation at the expense of long-term lung damage.[34]
Reward hacking	A proxy for the intended goal is used as a 'reward' and a continuously learning system finds an unexpected way to achieve the reward without fulfilling the intended goal.	An autonomous heparin infusion finds a way to control activated partial thromboplastin time (aPTT) at the time of measurement without achieving long-term control.[23]
Unsafe exploration	An actively learning system begins to learn new strategies by testing boundary conditions in an unsafe way.	A continuously learning autonomous heparin infusion starts using dangerously large bolus doses to achieve rapid aPTT control.[23]
Unscalable oversight	A system requires a degree of monitoring that becomes prohibitively time consuming to provide.	An autonomous subcutaneous insulin pump requires the patient to provide exhaustive detail of everything they have eaten before it can adjust the insulin regime.[33]

[249] Challen *supra* at note 3.

ATTACHMENT D

Supplement for

Select Applicable Legal and Regulatory Requirements

A. FTC mHealth Compliance Guidance

1. 2016 FTC Best Practices Guidance for mHealth App Developers (April 4, 2016) ("**FTC 2016 Best Practices Guidance**")

On April 4, 2016, the FTC issued this guidance document to provide privacy and security compliance best practices for mHealth App developers.

a. The best practices are divided into 8 categories:

(i) Minimizing collection and retention of data

Collect and retain only the data you need and take reasonable steps to secure the data transmitted and stored. Delete the data when no longer needed. Keep the data in de-identified form, keep up with technological developments concerning the risk of re-identification, and commit and contractually commit third parties, not to re-identify the data.

(ii) Limiting access and permissions

Do not access consumer information if not needed (e.g., a running app should not need to access the operating system's API for consumer information that is not needed for that functionality). Use trusted user interface components of the API where it makes sense to do so as those can provide more finely tuned access to only data needed for functionality of the app (e.g., have users select particular contacts to which to send text updates instead of accessing and using all contacts available through the API). Choose privacy-protective default settings that offer protection for users new to the technology while still accommodating the needs of more experienced users (e.g., set fitness app default to "private" rather than "public" so as to protect users from unwittingly sharing work-out results with others.

(iii) Keeping Authentication in Mind

Invest in design, implementation and testing of credential authentication. Consider multi-factor authentication to address substantial privacy risk circumstances (e.g., use of a password and a separate code sent via another channel such as an email or text). Require complex passwords and avoid use of default passwords unless consumers must change default during set up. Consider handling of requests to reset password, to revoke access to data (e.g., when device is lost), or close an account. Do not store passwords in clear text – add random data ("salt") so as to make it harder for cyberattacks. Limit access to your data or functionality (e.g., through API) to trusted users who have a legitimate need to access it.

(iv) Considering the Mobile Ecosystem upon which You are Relying

Research the variations in alternative mobile platforms and adapt your code as needed to protect the data regardless of those variations. Test the effectiveness of the security of the platform. Ensure that your third party service providers safeguard consumer data.

Include express and specific security requirements in the service contract. If using third party tools to build or enhance your app, ensure it conforms to your privacy promises to consumers and other consumer expectations. Test security vulnerabilities and real world applicability of the third party tool. Monitor the performance of the tool for vulnerabilities that can emerge from time-to-time.

(v) Implementing Security by Design - Develop a company "Culture of Security"

(a) Designate a trusted staff member to be responsible for data security.

(b) Build a security team of a size and mix of expertise that fits the company's size and complexity. Encourage transparency (disclosure and dialogue) and rapid response regarding security vulnerabilities.

(c) Incorporate data security at every state of the app's lifecycle: design, development, launch and post-market.

(d) This should include pre-launch testing and continuous monitoring, evaluation and updating. Testing should use real world scenarios.

(e) Use encryption at rest and in transit.

(f) Use stronger rather than weaker encryption methods and adapt them as standards change over time. Consider using proven, off-the-shelf encryption products rather than home-grown.

(g) Protect the app from common vulnerabilities (e.g., injection attacks, hard-coded credentials or cryptographic keys that hackers can exploit, insecure APIs that leak data or allow unauthorized access, broken or disabled cryptography). Consider using a rate limiting system to control network traffic so as to reduce the risk of automated attacks and multiple re-entry of passwords that can break into networks.

(vi) Stay Current.

(a) Have a plan for ongoing app updates and communication with consumers.

(b) Plan should include automatic updates and method for responding to identification of a significant security flaw.

(vii) Keep Track of collected and retained data.

(a) Maintain an up-to-date data inventory so as to allocate security resources as necessary and appropriate and to mitigate damage in the event of a breach.

(b) Know where all data from the app goes.

(c) Store sensitive data in locations with limited access.

(viii) Avoid Reinventing the Wheel

Use free and low-cost off-the-shelf security tools where possible, including those that help to provide encryption, conduct pre- and post-launch testing, test interfaces, scan networks for open ports, reverse-engineer programming code, check password strength and scan for vulnerabilities. (The FTC 2016 Best Practices Guidance document provides

several examples of sources.) Being Innovative in Methods for Communicating with Users; Obtaining User Consent and Providing Effective Notice

(ix) Methods of informing users about security and privacy options/features should be simple, clear and direct rather than including complicated jargon or hard to find links. Get affirmative consent (including indication of a "yes"), outside the context of the body of the privacy policy and terms of use, before collecting or sharing data, particularly health data.

(x) Provide **"Just in Time" Notice** to Consumers, regarding sensitive or unexpected data the app will collect – that is, both when the app is installed and again when the app begins to collect data.

(a) Consider explaining in the notice the reason why the app is collecting the data (so as to increase user understanding).

(b) Use icons, lights or other methods to alert users to availability of updates and to the fact that an app is currently collecting or sharing the data, as well as features (e.g., dashboards) that enable users to tailor privacy and security settings to their comfort level.

(c) Communicate to users the availability of enhanced security features (e.g., through a setup wizard, showcase security tools and instructions for use during initial user registration).

(xi) Have a privacy policy that is easily accessible through the app store (e.g., on a website that users can access from a computer with a large, readable screen, offering to email it, short policy with link to longer policy), clearly tells users what information the app will collect, and explains how the app will use, share and secure that data.

(a) Do not cut and paste the policy from another app.

(b) Do not forget to update the policy if your actual business practices change.

(c) Be mindful of other applicable laws

(d) Determine what other federal laws apply if health data will be collected.250

(e) Last and certainly not least, do not forget applicable state laws.

b. Other Related FTC Guidance Documents and Resources

(i) FTC public comments to the U.S. Commerce Department's National Telecommunications and Information Administration (NTI) on a draft template developed by a diverse group of stakeholders, and designed to be used by industry participants to communicate their

[250] *E.g.,* HIPAA (*see http://www.hhs.gov/hipaa/index.html (last visited June 13, 2016)*, FTC Act, FTC Breach Notification Rule (*see https://www.ftc.gov/tips-advice/business-center/guidance/health-breach-notification-rule (last visited June 13, 2016)*), FDCA (*see* discussion below of FTC April 2016 Tool). For other types of data, consider FTC truth-in-advertising principles (*see* https://www.ftc.gov/tips-advice/business-center/guidance/marketing-your-mobile-app-get-it-right-start and (both *last visited June 13, 2016)*), COPPA, and Gramm-Leach-Bliley and corresponding privacy rule (*see https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying* and *https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (both last visited June 13, 2016).*

policies on disclosing security vulnerabilities, particularly those in safety-critical industries (e.g., medical device and automobile manufacturers).[251]

(ii) Fed. Trade Comm'n, Cross-Device Tracking (January 2017)[252]

(iii) Fed. Trade Comm'n, Data Breach Response: A Guide for Business (September 2016)[253]

(iv) Fed. Trade Comm'n, Mobile App Developers: Start with Security (June 2015)[254]

(v) Fed. Trade Comm'n, Careful Connections; Building Connections in the Internet of Things (January 2015)[255]

(vi) Fed. Trade Comm'n, Start with Security: a Guide for Business (Lessons Learned from FTC Cases) (June 2015)[256]

(vii) Fed. Trade Comm'n, *Spring Privacy series: Consumer Generated and Controlled Health Data* (May 7, 2014)[257]

(viii) Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Change (March 2012)[258]

---

[251] *See* FTC Release *FTC Provides Comment to NTIA on Multistakeholder Initiative to Improve Cybersecurity Vulnerability Disclosure, https://www.ftc.gov/news-events/press-releases/2017/02/ftc-provides-comment-ntia-multistakeholder-initiative-improve* (February 16, 2017).

[252] *Available at* https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[253] *Available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.

[254] *Available at* https://www.ftc.gov/tips-advice/business-center/guidance/mobile-app-developers-start-security (last visited June 13, 2016).

[255] *Available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf (last visited June 14, 2016).

[256] *Available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.*

[257] *Available at* https://www.ftc.gov/system/files/documents/videos/spring-privacy-series-consumer-generated-controlled-health-data/ftc_spring_privacy_series_-_consumer_generated_and_controlled_health_data_-_transcript.pdf. At this program, the FTC Commissioner made clear that she considers CHI sensitive and in need of more careful handling than other types of consumer data. Presenters explored how the current regulatory environment allows for use and disclosure of potentially sensitive CHI in ways that consumers may not anticipate or understand and whether existing privacy frameworks are appropriate for protecting CHI. While the FTC seminar did not produce any specific guidance for businesses seeking to develop digital products involving CHI, the proceedings make clear that the FTC is and will continue to be watching this fast-growing segment of the digital economy.

[258] *Available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

c. 2016 FTC, OCR, ONC, FDA Collaborative Guidance on mHealth Apps – Interactive, Web-Based Compliance Tool ("**FTC April 2016 Tool**" or "**Tool**")

(i) On April 5, 2016, the FTC issued an interactive, web-based compliance guidance tool for mHealth App Developers. The FTC developed the tool in coordination with the Food and Drug Administration (**FDA**) and the Department of Health and Human Services Office for Civil Rights (**OCR**) and Office of National Coordinator for Health Information Technology (**ONC**). The Tool guides users through a series of high-level questions focused on the functionality of the app to information about applicable federal laws, including the FTC Act, the FTC Health Breach Notification Rule, HIPAA, and the Food, Drug and Cosmetics Act.

(ii) Of course, the Tool should not be relied upon exclusively in developing a compliance assessment and implementation strategy. The FTC's site itself includes a disclaimer that the Tool is "not meant to be legal advice about all of your compliance obligations, but it will give you a snapshot of a few important laws and regulations from three federal agencies."

(iii) The FTC April 2016 Tool guides users through whether the mHealth App is an FDA-regulated "medical device."[259] The Tool draws on and should be considered in tandem with prior, related FDA Guidance. However, the FTC April 2016 Tool adds an explicit, risk-based enforcement discretion criterion not present in the FDA MMA Guidance document discussed immediately above, asking: "Does your app pose 'minimal risk' to a user?" This criterion serves to exclude many apps from FDA oversight without the need to apply the MMA Guidance's somewhat difficult to apply definition of a mobile medical app.

d. Corresponding OCR Guidance

(i) OCR mHealth Web Portal (October 2015)

(a) OCR launched the mHealth web portal that allows mHealth app developers to get answers to their questions about HIPAA Rules and compliance requirements.[260] The portal is intended to encourage mHealth app developers to submit HIPAA-related comments and questions.

(b) In an email bulletin immediately following the launch, the OCR explained: "We are asking stakeholders to provide input on the following issues: What topics should we address in guidance? What current provisions leave you scratching your heads? How should this guidance look in order to make it more understandable, more accessible? The information gathered via the portal will also help the OCR develop future guidance covering mobile health apps.

[259] The Tool falls short of providing meaningful guidance concerning how and to what extent the FDA will regulate CDS, which is Software encompasses software and other tools intended to provide knowledge and patient-specific information, "intelligently filtered or presented at appropriate times," to assist in physician or patient decision-making. However, the December 2017 FDA guidance, "Clinical and Patient Decision Support Software" (CDS Draft Guidance) (December 7, 2017) describes how FDA intends to exercise oversight over CDS and patient decision support software

[260] *Available at* http://hipaaqsportal.hhs.gov/http://hipaaqsportal.hhs.gov/a/ideas/top/campaign-filter/active (last visited June 12, 2016)

(ii) OCR "Health App Use Scenarios and HIPAA" Guidance Document (February 2016)

Released prior to the 2016 FTC Tool in response to mHealth app developers' requests for additional guidance, this guidance document complements the OCR mHealth Web Portal with access to examples of when and how HIPAA applies to mHealth app developers in connection with a patient/consumer's creation, management, organization and/or transmission of his or her health information through the use of a health app (in particular, when they are considered acting "on behalf of" Covered Entities and are thus regulated as Business Associates).[261]

(a) Patient/Consumer downloads mHealth app to smartphone and inputs health data (e.g., blood glucose levels) s/he obtained from using home health equipment

Developer is not either a primary or downstream Business Associate. Patient/consumer is using the mHealth app without involvement of providers.

(b) Patient/Consumer downloads to smartphone mHealth app that helps her manage a chronic condition, downloads to her computer PHI through patient portal, and uploads it along with her own information to the mHealth app.

Developer is not either a primary or downstream Business Associate. Provider did not hire mHealth app developer to provide or facilitate a service on the provider's behalf.

(c) On physician's recommendation, Patient/Consumer downloads to smartphone an mHealth app to track diet, exercise and weight to help address a high BMI, and uses it to send summary report to physician for upcoming appointment.

Developer is not either a primary or downstream Business Associate. Physician did not hire mHealth app developer to provide or facilitate a service on the provider's behalf. Patient/Consumer's use of the app to transmit data alone does not make the developer a Business Associate.

(d) Patient/Consumer downloads to smartphone mHealth app that helps her manage a chronic condition. At Patient/Consumer's request, Provider and mHealth developer have entered into agreement to facilitate secure exchange of her health information between the EMR and the mHealth app. Patient/Consumer populates the app and directs it to transmit information to EMR so she can access test results through the mHealth app.

Developer is not either a primary or downstream Business Associate. Agreement to facilitate the exchange of the information alone does not create a Business Associate relationship because Patient/Consumer requested the arrangement. mHealth app developer is transmitting data on Patient/Consumer's behalf.

---

[261] *Available at* http://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/OCR-health-app-developer-scenarios-2-2016.pdf (last visited February 19, 2017). Examples previously addressed related to HIPAA compliance subjects such as text messaging, patient-generated data, information needed by Covered Entities to respond to OCR audits, business associate agreements, scope of the solution's environment that needs to be HIPAA compliant, online appointment scheduler solutions, de-identification, HIPAA training, security risk assessment tools, sale of PHI collected by a consumer-targeted app, use of third party API by EHR software partners, and HIPAA e-signature requirements. *See also* Mobile App Developers: Start with Security, *available at* https://www.ftc.gov/tips-advice/businesscenter/guidance/mobile-app-developers-start-security; Marketing Your Mobile App: Get it Right from the Start, *available at* https://www.ftc.gov/tipsadvice/business-center/guidance/marketing-your-mobile-app-get-it-right-start

(e) On physician's recommendation, Patient/Consumer downloads an mHealth app to a smartphone. Her provider has contracted with developer for patient management services, including remote health counseling, monitoring of food/exercise, patient messaging, EMR integration and application interfaces. Patient/Consumer-generated information is automatically incorporated into EMR.

Developer is a Business Associate of the Patient/Consumer's provider because the mHealth app provides the means for the developer to provide the provider the services under the agreement with the provider.

(f) Patient/Consumer downloads to smartphone mobile patient health record (PHR) mHealth app offered by Health Plan (a Covered Entity) to enable plan members to request, download and store health plan records and check status of claims and coverage decisions. The app contains the Health Plan's wellness tools for members to track health improvement progress. Health plan analyzes the information about app usage to understand effectiveness of the health and wellness offerings. The Developer offers separate, direct-to-consumer version of the app for Members/Consumers to personally store, manage, organize health records to improve health habits and send information to providers.

Developer is a Business Associate as to Member/Consumer's use of the Health Plan's wellness app. Develop is not a Business Associate as to Member/User's use of direct-to-consumer app.

B. Federal Communications Commission – Telephone Consumer Protection Act

1. The FCC's involvement in consumer privacy is grounded in the TCPA's prohibition against calls and messages to a mobile device using auto dialers and prerecorded messages from landlines without express written consent.[262] TCPA compliance has been and will remain an important focus for digital health companies in 2018, particularly mobile device application developers.

2. One persistent misconception is that the TCPA applies only to marketing phone calls or "spam" text messages, and that HIPAA covered entities and business associates are exempt from the TCPA. To the contrary, the TCPA applies to many automated communications between health care providers or health plans and patients, and the "safe harbor" established by the Federal Communication Commission for health-related text messages and phone calls is very difficult to meet.

3. Indeed, the TCPA presents a serious challenge for mobile device patient engagement tools, especially when violations of the TCPA can yield statutory damages of up to $1,500 per call or text message. While Federal Communications Commission orders over the past several years have added some clarity and a "safe harbor" for HIPAA-covered entities to help entities achieve compliance, there is still no "free pass" from the TCPA's requirements. Therefore, covered entities and the business associates who work for them should not assume that compliance with HIPAA offers any security of defense against a successful claim under the TCPA.

[262] 47 U.S.C. § 227 *et seq.;* 27 FCC Rcd. 1830 (2012); 45 CFR § 160.103 (2013); 47 CFR § 64.1200(a)(2) (2012); 47 CFR § 64.1200(a)(3)(v) (2012).

4. Strategies for Patient Engagement Tools

TCPA compliance is about identifying and managing risk in a way that does not hinder the benefits that these patient engagement tools can create for providers and patients alike. This requires consideration of several important questions when designing patient outreach programs using patient engagement tools, including:

a. What consent is required, and how will one be able to provide it was obtained?

b. What measures are needed to ensure that your vendors and other third parties comply with the TCPA when they make calls on your behalf?

c. How will a consumer's request to revoke their consent to receive calls and text messages be responded to and effectuated?

5. The TCPA prohibition received prominence in the healthcare context in *Mais v. Gulf Coast Collection Bureau, Inc.*,[263] a class action filed by a patient against a radiology provider and its billing agency and debt collection agent for debt collection calls to the patient's cell phone through a predictive dialer.

a. Both the district court finding in the plaintiff's favor and the Eleventh Circuit's reversal focused on the validity of a 2008 FCC Declaratory Ruling that providing a cell phone number on a credit application constitutes consent for subsequent medical debt collection calls.264

b. The district court had found the debt collector liable, holding that the declaratory ruling contradicted the clear meaning of the TCPA and that compliance with HIPAA is not tantamount to compliance with the TCPA. The Eleventh Circuit supported the validity of the ruling.[265] Particularly relevant to health care industry TCPA compliance planning is that the Eleventh Circuit characterized its decision that the TCPA permitted disclosure as consistent with HIPAA even though the plaintiff's cell phone number was included within the medical record information and thereby protected from disclosure under HIPAA.[266]

6. A non-emergency, non–telemarketing call subject to HIPAA made to a residential landline number generally is exempt from the consent, identification, opt-out, time of day and abandoned call requirements of TCPA.

7. FCC Order 15-72 (July 10, 2015)

a. Before Order 15-72 was released by the FCC on July 10, 2015 (July 10th Order), the same call to a wireless telephone number required (among other things) "prior express consent".

b. Under Order 15-72, providing a wireless telephone number to a HIPAA-covered Covered Entity or Business Associate constitutes prior express consent for a "health care" call or message within the "scope of consent given". Note, however, that:

---

[263] 768 F.3d 1110 (11th Cir. 2014).
[264] 27 FCC Rcd. 1830 (2012).
[265] 768 F.3d at 1119. The Eleventh Circuit ruled that that the district court lacked jurisdiction to address the validity of the 2008 FCC Ruling because any case challenging the validity of FCC orders must be brought directly to federal appellate courts under the Hobbs Act.
[266] *Id.* at 1125-1126.

(i) Not all calls made by a covered entity or business associate are exempt – only "health care" calls that are within the scope of consent (see below).

(ii) For purposes of Order 15-72, the FCC defines "health care" as it is defined under HIPAA at 45 C.F.R. § 160.103.

(iii) "Scope of consent given" is defined as: "closely related to the purpose for which the telephone number was originally provided." The FCC offers the following example: "…if a patient provided his phone number upon admission to a hospital for scheduled surgery, then calls pertaining to that surgery or follow-up procedures for that surgery would be closely related to the purpose for which the telephone number was originally provided…" (Order 15-72, fn. 474).

c. In its petition to the FCC, the American Association of Healthcare Administrative Management (AAHAM) specifically requested exemption for a "prescription notification" call or message that is "free" to the called party. The FCC granted this exemption.

d. While prescription notifications are exempt from the prior express consent requirement, most billing and many pre-approval calls and messages are not. Order 15-72 states: "[W]hile we recognize the exigency and public interest in calls regarding post-discharge follow-up intended to prevent readmission, or prescription notifications, we fail to see the same exigency and public interest in calls regarding account communications and payment notifications... While this second group of calls regarding billing and accounts may convey information, we cannot find that they warrant the same treatment as calls for healthcare treatment purposes. Timely delivery of these types of messages is not critical to a called party's healthcare, and they therefore do not justify setting aside a consumer's privacy interests in favor of an exemption for them. …"

e. Order 15-72 only exempts from the prior express consent requirement the following calls and messages: "calls for which there is exigency and that have a healthcare treatment purpose, specifically: appointment and exam confirmations and reminders, wellness checkups, hospital pre-registration instructions, pre-operative instructions, lab results, post-discharge follow-up intended to prevent readmission, prescription notifications, and home healthcare instructions" (collectively, Exemptions). The FCC specifically excludes (i.e., does not exempt from the prior express consent requirement) calls or text messages with "accounting, billing, debt-collection or other financial content".

f. Also, the Exemptions apply when a call or message is "free," i.e., does not "count against the [called party's] plan minutes or texts."

g. If a call or text message is within an Exemption, it still must meet other requirements of Order 15-72, which are:

(i) calls and text messages must be sent, if at all, only to the wireless telephone number provided by the patient;

(ii) calls and text messages must state the name and contact information of the healthcare provider (for voice calls, these disclosures would need to be made at the beginning of the call);

(iii) calls and text messages are strictly limited to the purposes [when there is exigency and the call has a healthcare treatment purpose]; must not include any telemarketing, solicitation, or advertising; may not include accounting, billing,

debt-collection, or other financial content; and must comply with HIPAA privacy rules;

(iv) calls and text messages must be concise, generally one minute or less in length for voice calls and 160 characters or less in length for text messages;

(v) a healthcare provider may initiate only one message (whether by voice call or text message) per day, up to a maximum of three voice calls or text messages combined per week from a specific healthcare provider;

(vi) a healthcare provider must offer recipients within each message an easy means to opt out of future such messages, voice calls that could be answered by a live person must include an automated, interactive voice- and/or key press-activated opt-out mechanism that enables the call recipient to make an opt-out request prior to terminating the call, voice calls that could be answered by an answering machine or voice mail service must include a toll-free number that the consumer can call to opt out of future healthcare calls, text messages must inform recipients of the ability to opt out by replying "STOP," which will be the exclusive means by which consumers may opt out of such messages; and

(vii) a healthcare provider must honor the opt-out requests immediately.

h. If a call or text message is not within an Exemption, then documenting prior express consent of each recipient for calls made or texts sent to wireless numbers is a key compliance step. The prior express consent does not need to be written (as it would be if the call or message contained any marketing or sales consent) but the sender bears the burden of proof. Also, the statute of limitations under TCPA is four years, which means consent records must be retained for no less than four years.

C. Overview of European Union ("Eu") Global Data Protection Regulation ("GDPR")

On May 25, 2018, the GDPR will become immediately effective and enforceable and will be the primary EU[267] law regulating the collection, use, safeguarding and disclosure of "any information relating to an identified or identifiable natural person" (*i.e.* a "Data Subject") ("PII"), including, without limitation, PII that fits within "special categories of personal data" that, by their nature, are particularly sensitive ("SPDs"). The GDPR replaces the EU Data Protection Directive 95/46/EC and is designed to update and harmonize data privacy laws across the EU to protect and empower individuals in the EU, and to reshape the way organizations with operations or customers in the region approach data privacy.

An "identifiable natural person" is broadly defined "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." In a clinical trial or other research, key coded data will remain PII if there are means reasonably likely to be used to re-identify the individuals who are the subjects of key coded data.

[267] As of December 22, 2017, the Members of the European Union include: Germany, Poland, the UK, Croatia, France, Spain, Italy, Romania, Sweden, Greece, Bulgaria, Czech Republic, Hungary, Austria, Netherlands, Finland, Belgium, Slovenia, Lithuania, Luxembourg, Portugal, Denmark, Malta, the Republic of Ireland, Estonia, Slovakia, Cyprus, and Latvia.

1. SPD categories of PII include:

a. PII revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

b. Genetic data, which means PII "relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question";

c. Biometric data, which means PII "resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data";

d. Data concerning health, which means PII "related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"; and

e. Data concerning a natural person's sex life or sexual orientation.

D. Application to "Controllers" and "Processors"

1. Definitions

The GDPR distinguishes between two types of entities: a "controller" is the entity that determines the purposes and means of the processing of PII, while a "processor" is entity that processes PII on behalf of the controller.

2. Extraterritorial Reach – Application of GDPR to Companies Outside the EU

a. The GDPR has direct extraterritorial reach to a controller and processor located in the U.S. or otherwise outside the EU ("U.S. Company") if it:

(i) Creates an establishment in the EU;

(ii) Offers goods or services (even if for free) to Data Subjects in the EU, such as by advertising in the EU;

(iii) Monitors the behavior of Data Subjects in the EU, such as by continuing to monitor patients after they return to the EU as part of, for example, post-discharge care.

Therefore, a company outside the EU that is targeting individuals in the EU will be subject to the GDPR.

The "offering of goods or services" is more than mere access to a website or email address, but might be evidenced by use of language or currency generally used in one or more EU member states ("Member States") with the possibility of ordering goods/services there, and/or mentioning customers or users who are in EU.

The monitoring of behavior will occur, for example, where individuals are tracked on the internet by techniques which apply a profile to enable decisions to be made/predict personal preferences, etc. This means in practice that a company outside the EU which is targeting consumers in the EU will be subject to the GDPR.

b. GDPR could indirectly apply to U.S. Company if it has contractual relationships with third parties who are subject to the GDPR.

3. General Principles

The GDPR requires both controllers and processors to process PII consistent with the following principles:

a. Transparency. The Data Subject must be aware of the nature, purpose and extent of the processing, including the risks and safeguards involved, along with their Data Subject rights.

b. Legitimate Purpose: Any processing must be compatible with a declared and specified purpose, which must conform to law, morals, and public policy.

c. Proportionality. Any processing shall be adequate, relevant, suitable, necessary, and not excessive in relation to the purpose.

Attachment E

Sample Contract Provision Addressing Key Privacy Compliance Considerations

In addition to its obligations regarding ABC Confidential Information set forth in Section X and elsewhere in the Agreement, Cloud Vendor acknowledges and agrees that: (a) it shall not reconfigure, de-identify, aggregate, sort, integrate, normalize, map, process, and/or combine with multiple disparate data sources (for comparison, benchmarking or other lawful purposes), or otherwise created derivative works from, any ABC Data, including, but not limited to, PHI or other personally identifiable information; (b) Cloud Vendor will provide ABC at no additional charge a copy of some or all of the ABC Data stored on the Cloud Vendor's cloud in a format reasonably requested by ABC at any time upon written request provided by ABC at least [XX] days prior to the date by which ABC wishes to receive the copy; (c) Cloud Vendor shall return or destroy some or all ABC Data as directed by ABC in its sole discretion at any time during the Term and upon termination of the Agreement; (d) Cloud Vendor shall not, and shall ensure that its and its Affiliates' partners, directors, officers, employees, contractors and agents do not, transmit, transfer, share, store, maintain, use, license, sell or disclose any ABC Data in any manner that: (i) constitutes a use or disclosure for purposes other than for Cloud Vendor's performance under the Agreement; (ii) would constitute a violation of Applicable Law, including, without limitation, HIPAA and other privacy and security laws and standards that would apply to use or disclosure of ABC Data by ABC; or (iii) that would involve the transmission, transfer, sharing, storage, maintaining, use, license or disclosure of ABC Data in any manner whatsoever beyond the boundaries of the United States, without ABC's prior written consent, which consent must be specific to the geographic area and specific entity to which the ABC Data will be provided; (e) ABC Data will be transmitted through only to and from the Cloud Vendor's Cloud in connection with the Agreement and only through interfaces that have been developed or provided by Cloud Vendor pursuant to the Agreement and accepted by ABC; and (f) Cloud Vendor is responsible for any use of ABC Data and ABC Confidential Information by Cloud Vendor staff.

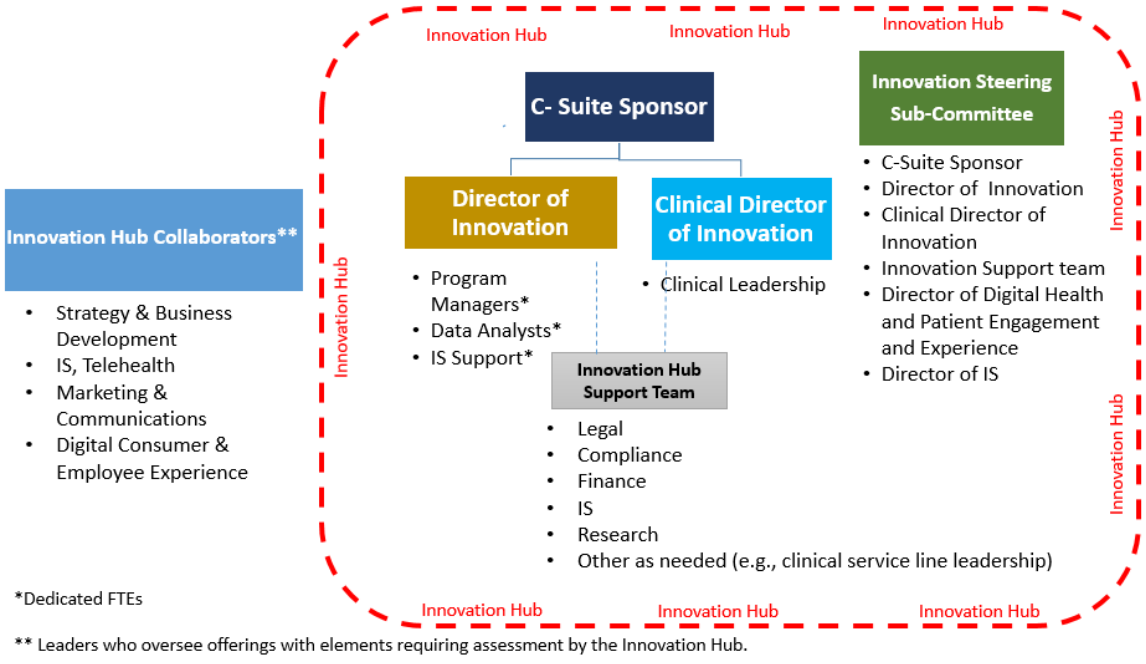
Attachment F

Representative Example of
Integrated Oversight of AI Innovation
Compliance Risk Assessment and Management

The following structure and process is presented as one possible approach for establishing a formal, well-defined pathway for the review and approval of AI and other technology innovation initiatives. It is intended to: (1) formalize the scope of responsibility and the membership of Innovation and Innovation investment oversight bodies, so it is clear to the organization where decision-making authority with regard to Innovation resides; (2) utilize clear and empowering delegation criteria to assign to the appropriate decision-making bodies the responsibility and authority to conduct initial intake and assessment and to recommend, and give final approval for, implementation of Innovation initiatives; (3) establish a single entry point for intake and assessment of proposed Innovation initiatives according to intake and assessment criteria, guidelines and policies; (4) facilitate timely and responsive guidance on the strategic, programmatic, financial, compliance, legal, technical, and other key aspects of Innovation initiatives; and (5) support ongoing monitoring of the various enterprise risks associated with Innovation initiatives.

A. Structure

1. The "Innovation Hub" as the Core Component of the Proposed Structure. As illustrated below, the "**Innovation Hub**" would be the core component of the proposed structure. The Innovation Hub would serve as a single point of entry and central and dedicated source for assessment of Innovation initiatives through a structure and process that would involve all essential expertise and resources in a fully integrated process for review and assessment of all relevant enterprise risks presented by a proposed Innovation initiative (including compliance risk). (See area within the red dotted lines in the diagram below.)



** Leaders who oversee offerings with elements requiring assessment by the Innovation Hub.

The key leaders encompassed within the proposed Innovation Hub would include the C-Suite Sponsor, a the Director of Innovation, and the Clinical Director of Innovation, who would manage and be supported by the Innovation Support Team Members who play a role in oversight of various categories of relevant enterprise risks. As described further below, the Innovation Steering Sub-Committee ("ISS") would be responsible for oversight of the Innovation Hub's key leaders and would provide higher-level executive involvement in making certain decisions that fall outside the scope of authority delegated to the Innovation Hub leaders. The Innovation Hub would integrate into its assessment and decision-making processes Innovation Hub Collaborators whose roles exist outside the Innovation Hub but who oversee offerings with elements requiring assessment by the Innovation Hub.

2. Oversight of Innovation Hub by Innovation Steering Committee. The ultimate responsibility for oversight of the Innovation Hub's assessment and decision-making would be vested in the "**Innovation Steering Committee**." One of the foundational acts of the Innovation Steering Committee would be to develop and approve the **Delegation Criteria** that define the scope of assessment and decision-making authority to be delegated to the Innovation Hub leaders (C-Suite Sponsor, Director of Innovation and Director of Clinical Integration) and to the Innovation Steering Sub-Committee. Decisions falling outside the scope of the authority granted in the Delegation Criteria would be referred to the Innovation Steering Committee. The Innovation Steering Committee would also develop and approve, for use by the Innovation Hub in exercising its delegated authority, the **Innovation Intake Criteria**, **Innovation Assessment Criteria** (which would address among other things whether the Innovation opportunity meets the legal and regulatory compliance standards embodied in the compliance program), **Innovation Equity Investment Criteria** and Data Exploitation Parameters, as well as such other substantive assessment and decision-making guidelines and policies as the Innovation Steering Committee considers necessary and appropriate to guide that exercise of delegated authority.[268] Possible members of the Innovation Steering Committee would include the C-Suite Sponsor and other select members of the executive leadership team such as the Chief Executive Officer, the Chief Human Resources Officer, the Chief Information Officer, the Chief Marketing Officer, the Chief Clinical Officer and the General Counsel. The Innovation Steering Committee will decide if and when other executive leadership should be engaged for consulting or decision-making purposes.

3. Role of the Innovation Investment Steering Committee. As illustrated in the Innovation assessment and approval process graphic shown and discussed in more detail below, the Innovation **Investment Steering Committee** would be tasked with reviewing Innovation projects with an Innovation equity investment component. The Innovation Investment Steering Committee could include the C-Suite Sponsor, the Chief Executive Officer, the VP Finance, the General Counsel, and an advisor from an Innovation-focused venture capital fund or investment bank with experience advising on technology innovation investment matters.

4. Delegation of Authority to the Innovation Hub. As noted above, the proposed Innovation intake, assessment and decision-making process would be driven and managed primarily by the Innovation Hub in accordance within the parameters set forth in pre-approved **Delegation Criteria**, **Innovation Intake Criteria**, **Innovation Assessment Criteria**, **Innovation Equity Investment Criteria**, **Intellectual Property Policy** and **Patient Data Commercialization Parameters**, as well as such other substantive enterprise risk assessment and decision-making guidelines and policies as necessary and appropriate to guide that exercise of delegated authority.

5. Allocation of Roles and Responsibilities within the Innovation Hub.

- The **C-Suite Sponsor** is a member of the executive team who would be ultimately responsible for (i) designing the overall innovation strategic plan and evaluating the intersection of this strategic

[268] These policies could be developed by the Innovation Hub (under the leadership of the C-Suite Sponsor) and may be implemented by the Innovation Hub Directors, the Innovation Steering Sub -Committee, the ISC or other committees (e.g., Data Request Committee).

plan with other strategic initiatives; (ii) overseeing the Innovation Hub's intake, assessment and decision-making; (iii) approving recommendations made by the Hub Directors (discussed below) if permitted by and consistent with established Innovation criteria, guidelines and policies; and (iv) engaging other individuals and oversight bodies within the broader review and approval structure and process as required by innovation policies or as the C-Suite Sponsor or the Innovation Hub leaders otherwise consider necessary and appropriate.

- The **Director of Innovation** would be generally responsible for the day-to-day oversight of the Innovation Hub's operations and personnel, design of the Innovation strategic plans and objectives, development of Innovation Approaches that advance such plans and objectives, and direct interaction with the C-Suite Sponsor on these and other Innovation Hub functions as appropriate. Together with the Clinical Director of Innovation (discussed below), s/he would review proposed innovation initiatives against the Intake Criteria to determine whether they qualify for further review and assessment by the Innovation Steering Sub-Committee. S/he would also manage the integration of the Innovation Support Team Members and Innovation Hub Collaborators into the Innovation Steering Sub-Committee's assessment process. In our experience, the Director of Innovation is supported by dedicated employees or contractors who provide, on either a full-time or part-time basis, general administrative, information systems/general technology, program management, and data analytics support.

- **Clinical Director of Innovation**. As in other health system Innovation Hubs in which we have been involved as legal counsel, the proposed structure would include a **Clinical Director of Innovation**. This position would be held by a licensed physician and play an essential role in: (a) the design, review, management, and oversight of all Innovation from a clinical management, patient safety, and quality perspective; (b) communicating with other clinicians about innovation strategy and initiatives; (c) assisting clinicians to design and implement Innovation initiatives in a manner that meets the applicable standard of care and protects patient safety (e.g., development of evidence-based protocols for innovation initiatives); (d) identifying and assessing clinical quality and safety risks associated with innovation initiatives (e.g., clinician reliance upon data generated from consumer healthcare tools); (e) reviewing existing policies, procedures, and protocols governing the delivery of healthcare to determine if enhancements are needed to integrate new Innovation tools; and (f) engaging with clinicians, professional associations, and community organization about the organization's innovation initiatives and other relevant topics (e.g., the extent to which technologies are supplementing and replacing services traditionally provided by clinicians). Together with the Director of Innovation, the Clinical Director of Innovation would review proposed innovation initiatives against pre-approved Intake criteria to determine whether they qualify for further assessment by the Innovation Steering Sub-Committee. The Clinical Director of Innovation would be a peer of the Director of Innovation with a direct reporting line to the C-Suite Sponsor and the Innovation Steering Sub-Committee so that the position has a level of authority and visibility sufficient to convey the importance of quality and safety considerations.

- The **Innovation Hub Support Team** members could include appointed representatives from each of the legal, compliance, finance, information systems, clinical service lines, and other departments who would dedicate a portion of their overall time to providing input and guidance to the Innovation Hub in their respective areas of expertise and responsibility on the design, assessment, implementation, oversight, and modification of innovation offerings as needed on an ongoing basis.[269] In particular, including representatives from the legal and compliance Departments on the Hub Support Team will allow for timely and effective input on potential Innovation legal and compliance risks. Of course, the individual members of the Innovation Hub Support Team would continue to be primarily assigned and report to the leaders of their respective departments.

[269] These appointed representatives would be individuals who understand innovation trends and associated risks, have the capacity/time to assist the Innovation Hub on a frequent, ongoing basis to review new and amend existing

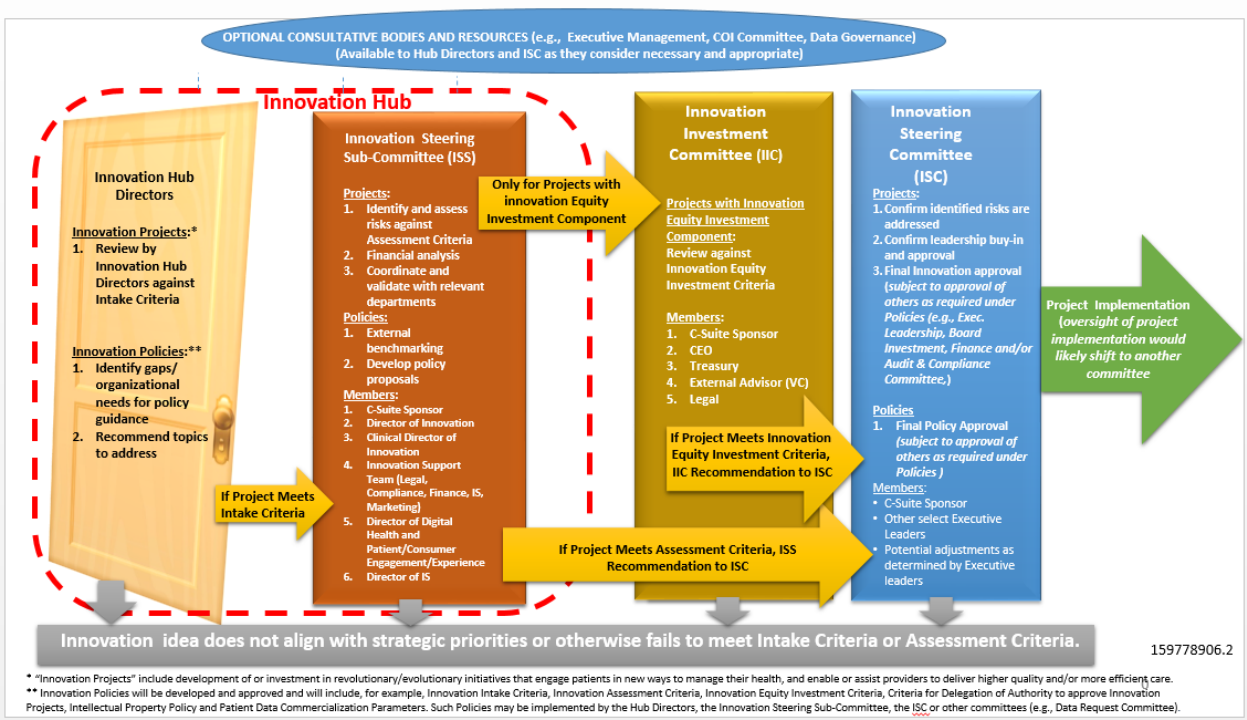
- The **Innovation Steering Sub-Committee** ("**ISS**") would consist of the C-Suite Sponsor, the Innovation Hub Directors, the members of the Innovation Support Team, the Director of Digital Health and Patient Engagement and Experience, and the Director of IS. It would undertake the assessment of innovation initiatives presented to it by the Hub Directors in accordance with pre-approved Assessment Criteria and approve them as and to the extent permitted by pre-approved criteria for delegation of authority. The Innovation Hub Directors are well-suited to co-chair the ISS. Matters decided here will not require review by the Innovation Steering Committee or the Innovation Investment Steering Committee); as a result, the ISS will be in a position to operate nimbly and pursuant to the Delegation Criteria set forth by the Innovation Steering Committee. As described above, the ISS is under the oversight of and reports to the Innovation Steering Committee.

- The **Innovation Hub Collaborators** would include other management personnel who design, manage, or oversee Innovation offerings with elements requiring assessment by the Innovation Hub, including Strategy and Business Development, Information Systems/Telehealth, Marketing and Communications, and the Digital Consumer & Employee Experience team. The Innovation Hub Collaborators exist outside the Integration Hub itself, but would be integrated into the Innovation Hub's activities so as to enable the Innovation Hub to better leverage the relevant expertise of the Innovation Hub Collaborators and better integrate the Innovation dimensions of the collaborators' roles and responsibilities into the overall innovation assessment, decision-making and oversight process.

B. Process for Intake, Assessment and Approval of Innovation Initiatives.

The graphic below illustrates one potential pathway for leveraging the centralized, integrated and focused Innovation Hub resources and oversight bodies to streamline the intake and assessment of new innovation opportunities and to create a formal and focused mechanism for review and approval of Innovation initiatives either within the Innovation Hub itself or, in some cases, within an organization's broader review and approval structure and process.

Innovation initiatives, and would be responsible for communicating/consulting with their respective departments with regard to the activities and needs of the Innovation Hub and for securing any necessary approvals from their respective departments.



The intake, assessment and approval of innovation initiatives illustrated above would include the following procedural steps:

***Step One*: Submission of Proposed Innovation Initiative through Innovation Hub as Sole Entry Point for Review and Assessment.** The Innovation Hub would serve as the single entry point for the submission of all potential innovation projects for review and assessment.

***Step Two*: Initial Review by Innovation Hub Directors against Pre-Determined Intake Criteria.** New innovation initiatives would be initially reviewed by the two Innovation Hub Directors under the direction of the C-Suite Sponsor against pre-determined intake criteria ("**Intake Criteria**"). If the proposed innovation fails to meet the Intake Criteria, the Innovation Hub Directors may decide to reject the innovation proposal at this stage or refer the matter to the Innovation Steering Sub-Committee as required or appropriate under applicable Intake Criteria or other innovation criteria, guidelines and policies.

***Step Three*: Review and Approval by the Innovation Steering Sub-Committee against Pre-Determined Assessment Criteria.** If a proposed innovation initiative meets the initial Intake Criteria, the Innovation Hub Directors in consultation with the C-Suite Sponsor would refer the initiative to the Innovation Steering Sub-Committee to undertake a further review against the Assessment Criteria. The Innovation Hub Directors may support the work of the ISS by involving one or more of the Innovation Hub Support Personnel and Innovation Hub Collaborators as necessary and appropriate. The ISS could approve the initiative if doing so would be authorized by the Delegation Criteria and consistent with the Assessment Criteria and other applicable innovation criteria, guidelines and policies approved by the Innovation Steering Committee, subject to obtaining any mandatory department-specific approvals (*e.g.*, Finance), and assuming the ISS does not feel the need to refer the matter to the IISC or ISC for further review.

The ISS would provide reports to the Innovation Steering Committee ("**ISC**") concerning what initiatives the ISS has approved and the ongoing progress in implementation of them. Such reports will support the ability of the ISC to stay well informed on innovation opportunities and risks, to evaluate the effectiveness of this integrated oversight structure, and to identify the need for potential enhancements to it that would improve the identification and management of legal, compliance and other enterprise risks.

As discussed above, some health systems have also created an Innovation Investment Steering Committee ("**IISC**") to review the special considerations involved in making investments in external innovation-focused companies. If there is a potential equity investment component to an innovation project advanced by the ISS, the IISC review would occur after review and clearance by the ISS but before review by the ISC. Initiatives approved by the IISC would still likely need ISC approval given the IISC's membership composition.

Step Four: Review and/or Approval by the ISC and the IISC (as applicable).

The ISC may authorize implementation of an innovation initiative, subject to obtaining any mandatory department-specific approvals (*e.g.*, Finance), if it determines that a proposed innovation initiative meets the Assessment Criteria, that IISC review and approval has been obtained where required or otherwise sought, and that no review or approval by any other decision-maker in the organization's broader management and governance structure is required or advisable.

The ISC would provide reports to such other decision-makers within the organization's broader management and governance structure concerning what initiatives the ISC has approved and their ongoing implementation. Such reports will support the ability of such other decision-makers to stay well informed on innovation opportunities and risks, to evaluate the effectiveness of this integrated oversight structure, and to identify the need for potential enhancements to it that would improve the identification and management of legal, compliance and other enterprise risks.

Step Five: Implementation. An innovation initiative may proceed to implementation if approved at any one of the review and assessment steps outlined above. Responsibility for the implementation of innovation initiatives would remain housed in the applicable health system departments outside of the Innovation Hub, and the Innovation Hub's role will shift to that of a support role. The Innovation Hub, including the Support Team members, will likely need to provide ongoing guidance and support to the departments responsible for implementation. For example, the representatives of the Legal and Compliance Departments who are serving as members of the Innovation Support Team could continue providing this important assistance/guidance during the implementation process and post-implementation as necessary to confirm the initiative is implemented and operated in a manner consistent with the Legal and Compliance Department's recommendations.

The responsible departments may need ongoing implementation assistance from other leaders and oversight bodies, such as (a) those with responsibility for implementation of programs and transactions once they are approved for implementation. Ongoing involvement of the Innovation Hub may also be needed to identify any requirements for managing risks associated with an approved implementation, and (b) those charged with responsibility for oversight and guidance on large strategic priorities and project benefit realization with regard to issues that arise during the implementation process, and measurement of the benefits of large-scale innovation projects.

Step Six: Continual Refinement of Process and Enhancement Opportunities. Once the Innovation Hub mechanism and the overall innovation program have matured and the structure and process outlined above has proven to be productive and effective, the scope of scope of approval authority delegated to the Innovation Hub Directors and C-Suite Sponsor, ISS and ISC in the Delegation Criteria may be expanded.

The Compliance Department and Legal Department would include in their regular reports to the management and board committee(s) responsible for oversight of legal and regulatory risk regular updates on the legal and compliance risk dimensions of innovation initiatives that have been reviewed within the Innovation Hub and ISC/IISC structure and process, including enhancements to the compliance program to better identify, assess and manage innovation-related compliance risks; the compliance risk exposure associated with approved innovation initiatives; and the effectiveness of the compliance program in managing/mitigating those risks on an ongoing basis under this integrated innovation risk management structure.