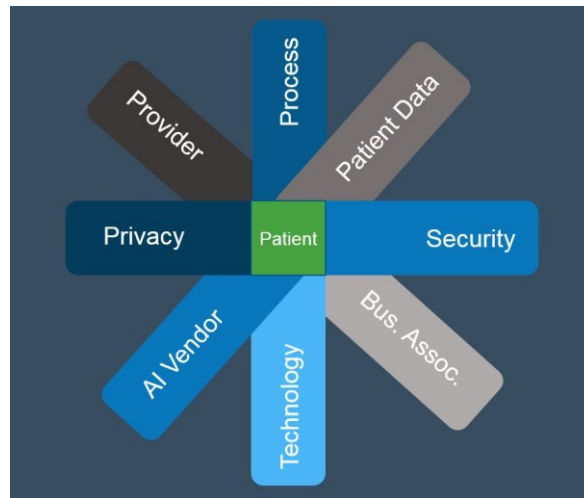


Data Empathy and AI (Part 1): The Need for a Patient Centric Analytics Ecosystem



As if, in the consolidation of an individual's data, we in healthcare could construct and embody a clone, built purely out of sensitive, personal, private data – a living, breathing person, a “Data Human,” that is how we must empathetically treat protected health information. Empathy is the capacity to understand or feel what another human is experiencing from within the other's frame of reference; i.e., placing oneself in another's shoes. A healthcare provider team must place itself in the shoes of the Data Human, just as if it was standing before them in flesh and bone. Data Empathy is just this – having deep and caring empathy for a patient's data, just as much as one would have empathy for the actual physical human being it represents. Blending Data Empathy into data management and security principles leads to a holistic approach to patient primacy and placing patients first, in the center of the healthcare ecosystem.

I. The Ecosystem in Healthcare and Related Problems

There is a very eclectic ecosystem that constantly shifts, blends, distorts and maneuvers through and around the theory of healthcare. At the center of this thriving, choking, sputtering and innovating ecosystem should be the patient, and the patient's Data Human. They are one in the same, yet either or both may be minimized or ignored in the practice of medicine.

Unlike most industries, there are a wide array of aligned and also non-cohesive parties, some of which have conflicting interests, within this healthcare ecosystem, by example: providers, every type and shade of vendor, including AI vendors, cloud providers, consultants, insurance companies and payers, government agencies, venture capital and angels, the patients and the Data Humans they represent and even the cyber criminals bent on stealing the Data Human. Whether there is a lack of coordination among providers, payers and HIPAA clearinghouses or other parties, or rampant incomplete datasets, the problems of bad data and lack of Data Empathy compound within the industry, driving the costs ever higher. Each of these parties and each of these problems has some impact upon the goal of patient primacy, upon the patient and the Data Human. Money and powerful special interests press in at the corners and infiltrate workflows and strategy, sometimes outweighing the primacy of patient care itself. And then we have the Data Human – the life blood of the provider and the patient; rich, intimate and highly valuable, always available to give, frequently asked “at what cost?” The patient must be at the center of this ecosystem, his or her rights, treatment and well-being uppermost in mind, particularly when innovation requires consumption of the Data Human. By looking at some of these concepts and players, the complexity of the ecosystem begins to emerge.

Cost Creep

We continue to watch the costs creep higher and higher against the backdrop of the GDP. There is no doubt that costs are and have been out of control and innovation is required to help with cost containment strategies. We know we need better outcomes, better quality and lower costs, and should be rewarded with better reimbursements in pursuing these goals. Yet the return of innovation has been slow at times in healthcare as costs continue to rise and data sets are consumed.

Emerging Technologies: AI

Technology like artificial intelligence (“AI”), as it emerges, may be loosely defined as the science and engineering of making intelligent machines, especially intelligent computer programs using different techniques, including models based on statistical analysis of data, expert systems that primarily rely on contingent statements, and machine learning. AI, at its core,

is software and data. AI may provide theoretical and practical solutions to the age old problem of cost, outcomes and quality. However, there is a lot of hype surrounding AI. In the aggregate, there is still very little return. Confusion abounds related to promise versus performance – stretch goals versus actual attainable goals. We need to cut through the noise and align the best opportunities to positively affect the patient, utilizing the most promising AI options that have yet to be realized. Challenges abound: adoption of AI in this quagmire of an ecosystem is a difficult process – the right guard rails are required – ethically, legally and in regard to data governance policy and workflows; taking actions based on analytic insights is still a challenge; translating insights into action is hard to do at the patient level and at population levels; how to blend data and put clinical, financial claims and operational and other data collectively to work still remains difficult; and lastly, ensuring proper investment in the horse that will win can be very speculative.

Regulations and Laws

There are obvious regulations that overlay healthcare; Stark Law, Anti-Kickback, False Claims, and HIPAA to name a few – all designed to tackle a particular aspect or behavior within the ecosystem. This limited article will focus mainly on HIPAA, by example, which serves to protect the privacy and security of individually identifiable information. Many state laws similarly give individuals certain rights of access and control with respect to their medical records and the information contained in those records. In general, however, ownership of the record remains with the provider who created or has custody of the Data Human and with that ownership comes custodial obligations.

The HIPAA Privacy Rule sets standards for individuals' privacy rights and how health information is used. It assures that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care – striking the functional balance permitting uses of information, while protecting the privacy of patients. The HIPAA Security Rule supports the Privacy Rule's prohibitions against improper uses and disclosures of PHI and focuses primarily upon reasonable controls to ensure the confidentiality (that e-PHI is not available or disclosed to unauthorized persons), the integrity (that e-PHI is not altered or destroyed in an unauthorized manner) and availability (that e-PHI is accessible and usable on demand by an authorized person) of PHI through administrative, technical and physical safeguards.

The issues related to privacy and security are not the only legal issues involved in the ecosystem. Without limitation, the following issues, both legally and ethically, will need to be considered: negligence and malpractice, respondeat superior and strict liability, as well as operational considerations hinging on legal notions such as bias and discrimination, proper documentation, evidence of proper development and testing, standards of care, causation, consent or authorization, burdens of proof and determination of fault.

Cybersecurity

Additionally, it is well known that the healthcare space is a rich hunting ground for cybercriminals, whether through ransomware or other attacks, hunting the Data Human. Direct and indirect combat erupts between a provider's implementation, maintenance and evolution of HIPAA principles, frameworks and information security controls and the cyber criminals themselves, who tend to move more nimbly than the defenders. Those organizations who have unfortunately fallen short of its compliance efforts, ending up on the HHS Wall of Shame or subjected to penalties, remind us constantly of the requirement to ensure the privacy and security of the Data Human. This needs to remain a key element in actually providing patient care (i.e., a provider cannot effectively care for a patient if it does not care for the Data Human).

Provider Permissible Use

Ultimately, one of the primary questions is whether the provider *can use the data* and for what purposes? This question touches on various controls including, by example, whether there is transparency conveyed in the Notice of Privacy Practice (“NPP”); whether the use is covered by an authorization or a consent, including the right scope; whether under a research study consent is waived; whether use or disclosure can be legitimately made without authorization. Once a compliant and authorized use is established, the next question is quite simply, *should the provider use or disclose this Data Human?* This question touches on several ideas including the ethical considerations surrounding such use. For example, based on the data ingested, is the machine making clinical decisions; what level of human intervention is at play; and whether reliance on such output poses additional risks for the patients. Again, ultimately, is the patient okay with, or is the patient expectation aligned with the use or disclosure of his or her Data Human in this manner – how transparent has the provider been in its explanation and does the patient understand the risks.

Scope of Data Use

Another consideration that flows from the above ethical considerations is “*what are we doing with data?*” In this context, assume that data under an AI algorithm feeds the engine for the desired output. Combining clinical, claims and other non-traditional data, for example, from wearable devices or mining social media, we can build a more comprehensive picture of the individual consumer which leads to more active participation in one’s health and wellness. With AI, the results are only as good as the software in combination with the data input. Hypothetically, as an AI tool continues to evolve, the goal would be that the results are better over time. AI must be intricately linked with humans who understand and can manage the technology. When employed properly, thoughtfully and humanely AI can make efficiency in burdensome processes, freeing up and retooling physicians to focus more on patients and outcomes, rather than on manual processes. AI can also knock out routine, non-serious issues that need to be handled quickly, accurately and inexpensively. As such, the scope of data use needs to be well thought out.

Larger Data Needs

There is also the very peculiar and prominent dilemma that has been vexing many industries related to its need to use more sophisticated analytics to run their businesses, which requires larger and richer sets of data. In healthcare, maturation includes focusing on blending clinical data with financial and other data to manage populations, accelerate clinical use cases, expand upon research capabilities and address problems across multiple provider disciplines. In the end, any strategy to ride the horse of analytics will require the use of this valuable and voluminous data, and the outcomes, again, are only as good as the data ingested and the reliability of the AI tool. Therefore, a symbiotic relationship between the usability and cleanliness of the data and new technologies that process this data must be established.

Patient Experience and Patient Engagement

As we innovate we also encounter unintended consequences – as technology rolls out, patient experience and patient engagement may be negatively impacted. Since AI is driven by large sets of data, data that needs to be input by clinicians, the less face time they have with patients and the more potentially subordinate that relationship becomes. AI can certainly agitate this relationship if not adopted with certain mitigation steps in mind, depending on the workflows, data needs, time to input data, etc. In general, healthcare, the industry that requires empathy more than any other, may actually lack that empathetic ingredient that should support trust within the encounter. We have seen where technology, a double edged sword, has made the practice of medicine more distanced from patients and has impacted patient experiences. Within the strain of healthcare systems to see more patients and provide better results, time and resources are stretched to the limit. It is increasingly difficult to offer truly personalized approaches to medicine. Yet some of the solutions to the problems vexing healthcare are found in personalization. AI may help offer more tailored approaches, but the cost to patient primacy must be paramount in this calculation.

Provider Process with Third Parties

Although this article gives just a summary into the ecosystem players, additionally, all of the third parties engaged by the provider or interacting with the Data Human must also be taken into consideration to understand the global impact on data from various channels. Again, there must be an all-inclusive governance and data management program guiding the organization and its employees in this regard. Further, all vendors, and in this context, AI vendors, cannot be engaged by a provider without first being vetted by the provider and thereafter establishing the appropriate contracts, terms and conditions and workflows with those vendors, whether they are business associates, contractors, or should be contracted under a data use agreement or other service agreement. Again, a patient’s most sensitive data is the centerpiece of AI activity, and when utilizing third parties, the provider is placing itself a step more remotely from the data itself, triggering the need to ensure that the AI vendors meet or beat their own security, privacy and internal policy standards. This means a provider’s legal group is and must be an integral team player in healthcare delivery.

Alignment of providers and vendors, the right processes and appropriately testing and vetted tools, is critical to the ultimate goal of providing better quality care at a lower cost. Questions that should be considered include: how much transparency is the patient afforded in the use of the Data Human and the management of health and wellness with third parties; how much of the Data Human is being used, disclosed and accessed by provider employees and also by third parties; and what additional governance has been established to support the use of these large sets of the Data Human by provider employees as well as third parties.

II. The Data Human and AI

When we blend together this ecosystem, we have daunting, complex problems. Patients and their Data Humans should be at the center of the solutions being built. New tools will need more of the Data Human in order to produce better results. How do we successfully account for all of these variances while build personalized solutions for patients?

Personalization

The “Personalization” of healthcare services can be attained through a carefully crafted blending of process, people and tools, ultimately strengthening the foundation of clinical care, and also leading to a more holistic relationship to the patients served. The starting point is the patient. At the core of the patient- caregiver relationship is the platform, not of technology, but of trust, which must be constantly nurtured. A provider cannot solve for patients if patients are not put first and in the center of the ecosystem. This means that a provider must build, not only the culture of caring, but also the culture of ensuring the ethical treatment and security of the Data Human. Any attempt at personalization that does not begin with this sentiment is a program that will eviscerate privacy.

AI Benefits and Risks to the Data Human

It is critical to know your patient and target individualized care accordingly. AI personalization benefits may include ensuring that we are addressing the right patients at the right time, as well as permitting, by need, caring for patients by the correct disciplines in order of most critical need. AI has shown that it can lead to better streamlined healthcare services and innovation in disease prevention. It fosters an inter-disciplinary team, changing the model for the practice of medicine, creating a more inclusive group of practitioners leading to efficiency, availability and quality of patient interactions. Further, current outcomes in general benefit future patients and continue to educate professionals, providing them with better/quicker tools. AI may therefore help with the ultimate goal of migrating healthcare away from being in the business of sickness to being in the business of wellness simply by the execution of its potential team effort approach and its constant education of those serving patients.

We need to keep in mind, however, the give and take with AI applications, including the fact that it may lead to less face time between a provider and patients. Balance in rolling out AI tools, therefore, is key. Someone has to enter the vast amounts of sensitive, rich data into the clinical tools, like the EMR, which can thereafter be ingested into AI tools. There is likely additional burdens on physicians as data entry tasks increase. As mentioned, this may lead to less face time and interaction with patients. The catch-22 is that, in trying to provide better care by using these AI tools, the primacy of patient care may diminish. Yet, another catch-22 remains at the heart of the AI challenge: the more data used, the higher the potential risk to privacy; yet, the less data used, the more risk to healthcare outcomes since the full patient picture may be unknown.

The Requirement: Patient Centric Ecosystem

Embedding analytic insights from AI directly into application, operational and clinical workflows is required to advance the notion of better quality and outcomes at a lower cost. However, the ecosystem in which this occurs must be patient centric and must include long term leadership commitment, patient experience and engagement, patient empathy, Data Empathy, robust security, thoughtfully implemented innovative tools, well vetted holistic platforms and contracts, a formal data governance framework to empower the rich data, and a team of teams approach to care coordination that includes a blending of legal, analytics, governance, clinical and security professionals. When the patient is locked in the center of this ecosystem, maturation of patient care through AI has its best hope of accomplishing the widest variety of goals, while maintaining the strictest level of patient preeminence.

Kevin Michael Mooney, Esq.
Senior Director, Enterprise Data Governance
The Cleveland Clinic Foundation
216-312-4887
mooneyk@ccf.org