DTSC 690 - FINAL PROJECT SCRIPT

OVERVIEW (SLIDE 2)

FIGURE 1. To help answer this question, we must first step back and look at the bigger picture. Personalized—or precision—medicine is a relatively new but significant approach to healthcare. Rather than using a one-size-fits-all method for diagnosing disease or prescribing treatment, it recognizes that each individual's genome is unique. What works for one person may not work for another. For far too long, this has been the approach of healthcare and providers. AI has transformed the landscape dramatically. This enables a more targeted and effective approach to care, benefiting not only patients, but also doctors, researchers, and communities as a whole.

AI precision medicine has unlimited potential, but there exists many ethical questions, including how a patient's data is gathered, manipulated and utilized, shared, sold or protected. While more clinicians and researchers are incorporating AI in their decision making for their patients, many patients lack awareness or are undereducated on informed consent as it relates to their genomic data. The concept of black boxes also shrouds how models arrive at certain conclusions, perplexing clinicians and researchers, as well as their patients.

OVERVIEW (SLIDE 3)

Within the context of personalized medicine, we'll focus on key themes including informed consent, data privacy and ownership, equity, and bias within AI models. Then, I'll briefly discuss the relevance of black boxes in AI and XAI, as well as the case of 23andMe and why it's important. Finally, I'll conclude with some prospective questions for future directions and research.

INTRODUCTION (SLIDES 5,6)

FIGURE 2. The time it takes to go from basic translational to clinical development and FDA review/approval can take almost a decade. With AI, we can cut that time frame in half, highlighting the importance of AI in healthcare, which will only evolve in the coming years.

FIGURE 3. There are several challenges that lie ahead in this space. First is the limited dataset currently available. Second, bias remains a concern in algorithms. Third, the black box dilemma where decisions that are output by ML are too complicated to understand. Lastly, all the guesswork from the process can be removed, leading to precision and personalized care and treatment therapies. That being said, the goal should be how can clinicians and researchers incorporate AI into existing frameworks without disrupting their normal flow of operations. And ensure that patients are involved every step of the way.

PATIENT AWARENESS AND INFORMED CONSENT IN AI-DRIVEN GENOMICS (SLIDES 8,9)

As AI evolves and becomes an integral part of our healthcare system, patients are, either knowingly or unknowingly, providing their genomic data for clinical and research use. Of course, the benefits are clear: the more diverse datasets we can gather the better. But are patients truly aware of and consent to how their data is used to arrive at certain clinical decisions? Without a doubt, these can dramatically affect patients' lives.

Remember the last time you were in the doctor's office or had to visit your local hospital. Do you recall signing necessary paperwork? Or did you just sign it because you were told to and were told it's required? That brings up the first point regarding informed consent. Is the process too difficult or complex to understand? Many patients wouldn't mind sharing their data, but are they fully aware of how it's used and/or shared? That being said, trust issues and/or misuse are

commonplace. How can patients trust a system they know nothing about? Who else will have access to the patient's data? Can they feel confident that their data will be protected and secured? What safeguards are in place?

FIGURE 4. In this figure, we see Gia, a chat-based AI tool, in action. It walks patients through the informed consent process regarding their genomic data. Gia accomplishes this through a simple and friendly conversation. It can answer basic questions and puts the patient in control. Gia and others that will follow help guide not only patients but clinicians and researchers on the importance of informed consent in an interactive format.

DATA PRIVACY AND OWNERSHIP IN PERSONALIZED MEDICINE (SLIDES 11,12)

As we've learned throughout our time in this program, AI and ML perform best when large datasets are available. Many times, people are asked to partake in a survey that asks about their income, hobbies, purchase history, education, etc. But the stakes are even higher when a patient's sensitive genetic data is involved. As the technology has evolved, so too have hackers and data breaches, prompting valid concerns of patient privacy and data ownership.

The consequences from having our genetic data abused or sold/shared without our consent could have widespread and lifelong effects. How can patients follow up and ensure their informed consent is limited? Is it possible to balance data privacy with AI innovation? Is there a way we can incorporate multi factor authentication/encryption which is becoming more commonplace these days, but instead with our sensitive genetic data?

FIGURE 5. In this figure, we see the breadth of privacy challenges plaquing patients. At every stage of the process, whether it's at the beginning where genomic data is collected to processing, sharing, and storage, that sensitive information is subject to privacy breaches and attacks. This highlights the importance of protection from unauthorized access to being able to re-identify an individual patient through data that was thought to be anonymized. We can see some ways in which AI can enhance security and protection including homomorphic encryption where data can still be processed and analyzed without having to be decrypted until the very end, and the concept of "Right to Be Forgotten" which many laws such as the EU's GDPR have incorporated, giving patients the opportunity to withdraw their informed consent and have their genetic data deleted from those systems.

TRANSPARENCY AND DATA SHARING IN AI-DRIVEN HEALTHCARE (SLIDES 14,15,16)

AI will only have a larger role in our healthcare in the coming years. We need to address a major ethical dilemma: Is it ethical that healthcare providers input their patient's genetic data into an algorithm, or "black box," that they aren't 100% sure how it exactly works? While it may provide an output based on the ML algorithm, is it still ethical to act upon those outputs? Would doctors risk not knowing how the algorithm arrived at their reasoning and follow through with the model output if it is able to save the patient's life?

Everyone involved needs to be mindful of the transparency and interpretability of AI-driven personalized medicine and patient's genetic information. Are physicians and patients alike aware of how the data is used or how the algorithm arrives at the recommendation they produce? Is there a way to verify, validate, or even challenge the output from the AI/ML model? All this prompts the necessary guidelines and frameworks required to make the process as transparent as possible. Explainable AI or XAI helps to reveal that black box once and for all.

FIGURE 6. It's a closed system where the user inputs some data and the model outputs its result. The box or model is either hidden or difficult to understand, e.g. why did this model produce this result? Why would a physician provide a medical recommendation to a patient without understanding or being able to challenge how AI came to that conclusion? Do the benefits outweigh the risks?

FIGURE 7. That's where Explainable AI or XAI come into play. Physicians may hesitate to provide medical advice or recommendations based on the black box in AI. XAI helps reveal the contents of that box. In personalized medicine, imagine a patient's cancer treatment. AI can suggest particular targeted modalities based on the patient's own genetic makeup. XAI takes it a step further and reveals the reasoning behind the AI output, e.g. a genetic marker discovered in the genomic sequencing. Rather than the patient and physician going through trial and error, especially in cancer where time is extremely limited, targeted modalities could save time, money, and possibly the life of the patient. In short, XAI helps AI models become more transparent and easier to understand.

EQUITY AND BIAS IN AI MODELS FOR PERSONALIZED MEDICINE (SLIDES 18,19)

While we focus on the big picture and the end goal - using AI models in personalized medicine - we also must be mindful of the inequities and biases that are present with relation to data collection, data processing, and data analysis. It would make sense then that if the input data is biased, the output would be biased as well. These disparities even exist outside the realm of AI/ML, but AI/ML can reveal or expand upon such disparities, especially minority groups and those in underrepresented communities. Even if there are good intentions, the final product may not be well-intentioned. We must understand that in human nature, there are inherent biases, but how can we develop algorithms to remove these biases? That's clear in regular/traditional medicine today. How can we improve the condition by involving all stakeholders, e.g. physicians, patients, policymakers, and community activists? Even if the input is biased, how can we ensure that the output is unbiased and represented by the whole population?

FIGURE 8. In this figure we can see how biases in training data can significantly and detrimentally affect certain populations. Even if the AI algorithm/ML model is unbiased and applied across diverse groups, the output would be flawed and misleading.In the case of prostate cancer, populations with lower risk may be flagged as positive whereas populations with higher risk may be flagged as negative. This figure highlights the importance of recognizing and addressing these biases to ensure AI tools in personalized medicine are fair and accurate.

CASE STUDY - 23ANDME (SLIDE 21)

I will preface by saying that I am or rather was a customer of 23andme and was affected by the breach and recent bankruptcy. The data breach in 2023 not only exposed patients' genetic information, but it revealed flaws in the company's safeguards. This year, the company filed for bankruptcy, which caused widespread frustration at the company directly and concerns for what happens next to their genetic data.

When initially prompted, were patients aware of what could happen to their data in such circumstances? Mostly likely not because they didn't expect something like this to happen. How many people read the Terms of Service or the fine print? And once something did happen, it was too late. The process to control, manage, or even delete one's genetic information was complex and convoluted. This should definitely not be the case.

What can we learn from this case study? Patients should be given the opportunity to choose the level or extent to which their data is used, stored, and shared or ultimately shared/sold in this particular case as a condition for business sale. Would it be possible to prevent such events from happening in the first place if stronger protections and safeguards were already in place? Should companies that manage our genetic information be scrutinized to a greater extent by other independent doctors, researchers, policymakers, and industry leaders?

CONCLUSION (SLIDE 23)

SUMMARY

Informed Consent. With regards to AI and personalized, it's imperative that patients are informed of how their genomic data will be used and consent is obtained.
Privacy and Security. More so than perhaps in any other field, there needs to be stronger safeguards as it relates to a patient's sensitive genetic data so that information isn't misused or accessed by unauthorized users.
Transparency. While doctors and clinicians aren't required to understand the exact code or algorithm that goes into their AI/ML models, they should understand why a certain recommendation was produced by the model. This allows healthcare providers and patients alike to trust the process a bit more.
Bias and Equity. Biases, inequalities, and disparities are inherent in human nature. But it can be amplified exponentially as it relates to AI in healthcare. If this issue is not addressed, it will lead to false negatives/positives in diagnoses and delays in obtaining the right treatment, which could cost patients their lives. That would only further the biases, inequalities, and disparities already prevalent in our society today.

FUTURE DIRECTIONS

Informed Consent

Question: How can we improve patient understanding of AI-driven decisions involving their genomic data?
Recommendation: Develop interactive, chat-based consent tools like Gia. Patients are informed, can ask questions, and provide their consent.

Privacy and Security

Question: What new technologies can ensure data privacy without compromising model performance, especially in personalized medicine?
Recommendation: We already discussed homomorphic encryption, but there are others, including differential privacy which purposefully adds some noise to the dataset without compromising the identities of individuals/patients, and blockchain, a decentralized system that allows for increased security and transparency, so that no single party has all access to the information.

Transparency

Question: How can we increase clinician and patient trust in black-box AI systems?
Recommendation: We addressed this in depth with Explainable AI (XAI), which is only going to evolve further. Personally, I hadn't come across the term XAI until this project, but it makes perfect sense when doctors can feel confident in their medical recommendations and patients are aware of how AI is incorporated into their personalized care.

Bias and Equity

Question: How do we identify and reduce hidden biases in AI models trained on genomic and clinical data?
Recommendation: Require datasets that are both diverse and underrepresented in model development and deployment to promote fair and equitable results.

DTSC 690 - FINAL PROJECT SCRIPT

WORKS CITED (SLIDE 25)

1. Bernal, Jose, and Claudia Mazo. "Transparency of Artificial Intelligence in Healthcare: Insights from Professionals in Computing and Healthcare Worldwide." Applied Sciences, vol. 12, no. 20, 2022, article 10228, https://doi.org/10.3390/app122010228.
2. Carini, Claudio, and Attila A. Seyhan. "Tribulations and Future Opportunities for Artificial Intelligence in Precision Medicine." Journal of Translational Medicine, vol. 22, 2024, article 411, https://doi.org/10.1186/s12967-024-05067-0.
3. Dankwa-Mullan, Irene. "Health Equity and Ethical Considerations in Using Artificial Intelligence in Public Health and Medicine." Preventing Chronic Disease, vol. 21, 2024, http://dx.doi.org/10.5888/pcd21.240245.
4. Fothergill, B. Tyr, et al. "Responsible Data Governance of Neuroscience Big Data." Frontiers in Neuroinformatics, vol. 13, 2019, https://doi.org/10.3389/fninf.2019.00028.
5. Hanna, Matthew G., et al. "Ethical and Bias Considerations in Artificial Intelligence/Machine Learning in Pathology and Laboratory Medicine." Modern Pathology, vol. 38, no. 3, 2025, article 100686, https://doi.org/10.1016/j.modpat.2024.100686.
6. Holthouse, Ryan, et al. "The 23andMe Data Breach: Analyzing Credential Stuffing Attacks, Security Vulnerabilities, and Mitigation Strategies." arXiv, 2025, https://arxiv.org/pdf/2502.04303.
7. Karim, Md. Rezaul, et al. “Explainable AI for Bioinformatics: Methods, Tools, and Applications.” arXiv, 2022, https://arxiv.org/abs/2212.13261.
8. McGuire, Amy L., et al. "Research Ethics and the Challenge of Whole-Genome Sequencing." Nature Reviews Genetics, vol. 9, no. 2, 2008, pp. 152–156, https://doi.org/10.1038/nrg2302.
9. Mittal, Aayush. "The Black Box Problem in LLMs: Challenges and Emerging Solutions." Unite.AI, 1 Dec. 2023, www.unite.ai/the-black-box-problem-in-llms-challenges-and-emerging-solutions/.
10. Park, Hai Jin. “Patient perspectives on informed consent for medical AI: A web-based experiment.” Digital health vol. 10 20552076241247938. 30 Apr. 2024, doi:10.1177/20552076241247938.
11. Savage, Sarah K., et al. "Using a Chat-Based Informed Consent Tool in Large-Scale Genomic Research." Journal of the American Medical Informatics Association, vol. 31, no. 2, 2024, pp. 472–478, https://doi.org/10.1093/jamia/ocad181.
12. Yang, Guang, et al. "Unbox the Black-Box for the Medical Explainable AI via Multi-Modal and Multi-Centre Data Fusion: A Mini-Review, Two Showcases and Beyond." Information Fusion, vol. 77, 2022, pp. 29–52, https://doi.org/10.1016/j.inffus.2021.07.016.
13. Zhou, Juexiao, Chao Huang, and Xin Gao. "Patient Privacy in AI-Driven Omics Methods." Trends in Genetics, vol. 40, no. 5, 2024, pp. 383-386, https://doi.org/10.1016/j.tig.2024.03.004.