Title :
Ethical concerns in digital health monitoring system

By

011222215 - Toufiq Ahmed
011222321 - MD.Nahianul Joha
011222279 - Sabbir Ahmed
011222203 - Md.Saharier Iqbal
011222259 - Fariha Nizam Prova
011222342 - Mardia Yasmin Muna
0112320065 - Md. Tanvir Ahmed
0112320187 - Md. Farhadul Islam

Submitted in partial fulfilment of the requirements
of the degree of Bachelor of Science in Computer Science and Engineering

December 20, 2023

Department of Computer Science and Engineering
United International University

Abstract

Digital health monitoring systems are transforming the medical field, but their implementation raises ethical concerns regarding fairness, equity, privacy, and potential biases. Future healthcare professionals must be equipped to address these challenges and ensure that digital health advancements benefit all individuals. While digital health holds immense potential to revolutionize healthcare delivery, its design and implementation require careful consideration to avoid exacerbating existing disparities and promoting ethical practices. The integration of loT technologies in smart healthcare systems offers significant advantages, but it also presents new ethical challenges related to data security and privacy. Developers, users, and governments must collaborate to balance user experiences with robust ethical safeguards to ensure that the benefits of these technologies are shared equitably and responsibly. In this article, we will discuss the complexities that come with using technology in healthcare, such as wearable trackers and apps. It examines these issues from various perspectives, such as those of patients, doctors, and society as a whole. Finally, we attempt to propose some potential solutions.

Acknowledgements

This work would have not been possible without the input and support of many people over the last two trimesters. We would like to express my gratitude to everyone who contributed to it in some way or other.

First, we would like to thank my academic advisors, ...

Our sincere gratitude goes to ...

We are also thankful to ...

Last but not the least, We owe to our family including our parents for their unconditional love and immense emotional support.

Table of Contents

Chapter 1

Introduction

The convergence of cutting-edge technology and healthcare has ushered in a new era of medical practice, with digital health monitoring systems reshaping how we approach wellness and patient care. These systems, which are powered by the convergence of wearable devices, data analytics, and real-time connectivity, have the potential to take healthcare delivery to new heights. They provide individuals with information about their own health statistics, promote proactive management of health, and provide healthcare professionals with data-driven decision-making capabilities. Nonetheless, an intricate web of ethical concerns develops amid the optimism surrounding these innovations, necessitating meticulous examination to ensure that the integration of technology aligns harmoniously with the values that strengthen the medical field. The promise of digital health monitoring systems is centered on empowering individuals to take charge of their health. These systems deliver an ongoing flow of data ranging from vital signs to behavioral patterns, allowing users to be proactive in their wellness journey. This new level of patient engagement has the potential to transform preventive care, improve early diagnosis, and foster a greater sense of control over one's health. This transformative potential, however, is accompanied by several ethical challenges that require careful consideration. Among these concerns is the complicated issue of data privacy and security. The data collected is naturally sensitive and valuable due to its nature, which ranges from personal health information to lifestyle behaviors. The ethical challenge is to capitalize on the insights gained from this data while maintaining the utmost respect for individual privacy and ensuring robust security against breaches and unauthorized access. However, this revolutionary potential is accompanied by several ethical challenges that must be carefully considered. The complicated issue of data confidentiality and safety is one of these issues to consider. Because of its nature, the data collected is susceptible and essential, ranging from personal health information to lifestyle behaviors. The ethical challenge is to capitalize on the insights gained from this data while respecting individual privacy and ensuring adequate safety against violations and unauthorized manipulation.

Chapter 2

The Ethical Problems

2.1 Truthful information, empowerment, and informed consent:

In arrange to form individuals competent to utilize the openings advertised to them in case they wish, honest data approximately the benefits and dangers of engaging in computerized well-being strategies should be given to the person clients. Thus, clients ought to be persuaded and enabled (in an enlightening as well as specialized sense) to lock in advanced well-being innovation. For this, open communication, specialized preparation, and instruction ought to be offered. It is critical that their interest is intentional and isn't undermined by any sort of motivating force, be it of a budgetary nature or prioritizing those that utilize computerized well-being innovations when they look for restorative care in non-digital, customary healthcare settings. Not utilizing these openings may not be authorized or result in a need get to to wellbeing administrations. Additionally, 'users' should be mindful that their information is being collected for health-related purposes, for occasion within the case of area tackers, which can deliver data about an individual's wellbeing (e.g. when visit visits to healing centers or other healthcare destinations are reported). However, for open well-being purposes, total data, e.g. from social media posts approximately flu side effects, seem to deliver hints of the spread of diseases—techniques being alluded to as advanced the study of disease transmission and scourge estimating. In common, in any case, there's the peril of advanced well-being building up an observation society. This and other challenged employments ought to be precluded by law and anticipated in the hone.

As respects honest data, educated assent also plays a major part. Though traditional models of educated assent pointed to illuminate patients and investigate subjects and fundamentally centered on maintaining a strategic distance from hurt to the person within the course of the procedure—thus having a constrained period—new models of educated assent for computerized wellbeing got to be considered. Those unused models ought to not as it were take into consideration expecting and unintended employments of information given by mindful clients, but ought to consider the bigger time measurement when infor-

mation is put away (and possibly utilized) for a significant sum of time. Moreover, certain sorts of computerized well-being, e.g. when hereditary information is included, expand the information picked up approximately a person to his or her hereditarily related family individuals. Amendment of existing and conventional models of educated assent, such as opt-out, waiver, no assent, and open or categorical assent, is required for assembly of the challenges posed and altering assent instruments appropriately to guarantee and advance independence for everybody in line with reasonable information uses.

2.2 Ambiguities in the laws:

Scenario: Visualize a future in which wearable technology of the highest caliber is incorporated into commonplace devices. These devices gather data about people's vital signs, levels of activity, and even their emotional moods in real-time. For individualized medical care, illness prevention, and even workplace safety, this data is priceless. However, the murky legal environment surrounding data privacy raises a serious ethical question.

The Ambiguity: Although several laws protect people's medical information, others let employers, insurance providers, and even law enforcement access to it in certain situations. There is a growing blurring of the boundaries between issues of public health, private health, and potential discrimination based on health information.

Moral Conundrums:

Informed permission: If rules are unclear or change quickly, how can people give informed permission if they are not aware of all the possible uses for their health data?

Data Ownership and Control: Who is in charge of the medical records that these systems gather? People, businesses, or the government? Who is authorized to use, distribute, or even remove this data?

Bias & Discrimination: Can people be unfairly discriminated against based on their genetic predispositions, lifestyle choices, or state of health? This gives rise to questions regarding insurance premiums, work prospects, and even public service accessibility.

Misuse and Manipulation: Health information can be abused for government surveillance, social engineering, and targeted advertising if it falls into the wrong hands. How do we make sure that there are strong defenses against these kinds of rogue apps?

Possible Repercussions:

Loss of Trust: People's confidence in healthcare institutions and digital corporations may drastically decline if they believe their personal health information is not secure or is being exploited against them.

Chilling Effect on Personal Health Monitoring: If people worry that their data can be exploited, they might be reluctant to use these potentially life-saving devices.

Expanding Health Inequalities: Communities that are underprivileged and are more susceptible to data exploitation may suffer disproportionately from vague legislation.

2.3 Risk from social network

Robust social networks increase the difficulty of maintaining privacy since private information can be shared without the owners' permission. Social networking is the first place that young people, in particular, go for answers (Denecke et al, 2015). It is challenging to hold certain healthcare providers accountable if patients disclose their personal information on social media. Furthermore, certain operators offer their own social networks where users can share information and consult with one another, support one another, and other functions. Even while they can become friends on social media, if a disagreement reaches a higher level and exposes sensitive information or the leakage of personal data, the results for privacy and personal life may differ.

Chapter 3

Ethical problem and challenges

3.1 Challenges for Healthcare Organizations:

The expense of technological devices is one of the major obstacles for organizations in terms of setup and afterward upkeep. The failure to straightforwardly evaluate the elusive patient and money-saving advantages makes it hard to esteem, and hence legitimize, the capital consumption on innovation. Compared to more widespread installations, remote monitoring may be considered a compromise. It is argued that reducing unnecessary hospital use can help cut healthcare costs, which may be especially important when managing chronic diseases. From a practical point of view, this is advantageous in terms of maximizing effective outcomes for as many patients as possible. However, the literature suggests that remote monitoring does not reduce costs for the vast majority of people. From the point of view, this is useful in expanding successful results for whatever number of patients could reasonably be expected. Therefore, the majority of the research suggests that remote monitoring does not reduce costs. Most investigations recommend insignificant, if any, cost reserve funds, and some of the time inflated costs; However, for the treatment of chronic conditions, positive clinical outcomes were reported. The idea of 'new' innovation raises the issue of interoperability. Due to the timescales involved, the combination and cross-access of information and utilization between different frameworks or even different adaptations might be difficult. It could be argued that this goes against the ethical obligation of organizations to ensure that the integration of legacy systems meets integration standards, which comes from their fiduciary relationship with patients.

3.2 Challenges for Healthcare Providers:

Specialists have referred to the "drawing" of the need to provide the best clinical thought as the source of moral issues during clinical interactions. This is because it suggests using the most cutting-edge and up-to-date care. The social cycle that makes sense of why the meaning of another biomedical development changes, as individuals become accustomed to its use, may begin with how new clinical benefits levels of progress are considered.

The control of the region is crucial when considering economies of scale as a component of progress. Specialists should get full help in the state in which the patients stay in the US and the European Collusion. In the different cases to this point, it has been spread out that clinical idea specialists are "wandering" to the patient for the virtual improvement of clinical ideas, requiring a license for that state. Additionally, Beauchamp cared for Childress. The ethical standard of "Basic worth" for gaining respect in the thriving asset sector, as defined by the Four Standards framework, can without a doubt be transformed into a true commitment to not deny patients consent to the most advanced considered care due to their geographic location. Despite the gigantic entrances introduced by clinical benefit improvement, ill-advised execution should be redirected. The mechanical objective demonstrates the need for social marvel by suggesting that the new movement and its essential nature be confirmed. The patient is "(the) fight zone and (the) prize" in the clinical industry, where progression appears to be shifting the focus from prosperity and recovery under reliable independence to death. Using a reliable patient to meet the wrap-of-life hypothesis raises an ethical issue since it abuses one of the clinical moral quality's most enormous focal convictions: Autonomy. We need to take a gander at how significant quality began to look into this.

The boss's proposal is a crucial decision with no room for change. Experts could hardly refuse to manage the treatment because of this. Therefore, the moral major derives from a social affiliation that intervened early enough that, even though novel development is not recommended, the principal brings about expectedness as a result of routinization and is unambiguous about how the social milieu has affected the interpretation of its sufficiency.

3.3 Challenges for Patients:

Problems for patients the moral fundamental's effects spill over into problems for patients themselves. The need to guarantee fitting use of costly stuff (regardless during the early assembling stage) and the ethical objective to use the new improvement stays as a speedy test to the need to shield patient independence, as gotten from the use of personalism to clinical thought structures. Their original worth, which consolidates normal attributes like the opportunity of thought, is their sign. Participation in decisions that impact them might perhaps understand their causative potential. Thus, inside the patient-focused structure of contemporary medication, the test of the ethical basis is an immediate infringement. However, innovation need not be constrained to a false dichotomy between the worth-ladenness theory and the worth-nonpartisanship theory. Our convenience to the imaginative objective and loss of freedom is not exactly proposed by the insistence of mechanical worth. Innovation's inborn characteristics, which compare to human instinct's defects, give it esteem, as indicated by Cassell. Similar to how treating the value-laden nature of development necessitates the organization of our characteristics and self-control, treating its ethical problems necessitates the organization of our ethos. Despite keeping an eye on the particulars, it is essential to take into consideration the significant issue

of patient permission for cutting-edge clinical benefits advancement and organizations. From a utilitarian point of view, whether, for instance, remote observation increases access; We are aware that the majority of these access upgrades have not been accounted for. Additionally, the information into whether distance truly investigating advances more undeniable access for the most defeated gives a comparable outcome in that the Rawlsian point of view isn't satisfied [16]. With cutting-edge well-being innovation programs, it is feasible to characterize the troubled as the underserved. Instances of these gatherings incorporate detached networks, local organizations, and unambiguous social events of the populace in light of the monetary hole. Far-off associations, a significant part of the opportunity arrive up short on key cash-related and inventive foundations while the authentic improvement might be lopsided to those with great degrees of creative tutoring. This is, obviously, under the presumption that the tremendous

In any case, improvement has been offered or conveyed.

Ethics by the plan is as yet an essential thought for the arranging time of electronic clinical benefits development. Stop access segregation, forces engineers to plan with moral implications in mind.

Chapter 4

Solutions

During the utilization of digital health :

4.1 Fairness in storage:

In the utilization of digital health technologies, ethical challenges arise concerning the storage, access, sharing, and ownership of data, as well as the disclosure of results. These challenges impact the fair use of digital health, encompassing security, privacy, confidentiality, discrimination, unintended data uses, and the right to know or not know results, including incidental findings. During the storage phase, precautions must be taken to prevent unauthorized access, such as hacking, to avoid discrimination and stigmatization. When granting access to stakeholders, considerations of fairness arise, questioning the purpose, benefits for stakeholders, commercial objectives, user awareness, and intended versus unintended uses. Addressing these questions is crucial for ethical issues like autonomy, informed choice, and the right to privacy. A fair use of data also involves determining ownership and custodianship. While universal regulations are lacking, safeguards are needed to prevent the exploitation of individuals who donate their data. It remains to be defined who should benefit financially from donated data and under what conditions while ensuring public welfare benefits. Digital health, according to Topol, supports the 'democratization of medicine,' providing individuals with increased access to their medical information for autonomous health management. However, caution is needed to prevent overburdening those who may struggle to manage their health.

4.2 Dignity and Autonomy:

Furthermore, the application of digital health tools should be contingent upon preserving the dignity of the patient. For example, when employing telemedicine within hospital settings, the communication of potentially distressing information to the patient should align with maintaining the patient's dignity. Consequently, the use of distant technologies, such as screens, should be avoided when delivering news that places the patient in

a vulnerable situation. Instead, prioritizing personal and face-to-face communication is recommended to safeguard the dignity of patients in such vulnerable scenarios. However, autonomy, in terms of allowing patients to choose the communication channel, can play a role in tailoring healthcare delivery to the individual needs of patients. Conversely, for patients who prefer not to be institutionalized, the use of telemedicine enables them to stay at home for an extended period, receiving better support in their home environment. This application of technology can enhance their quality of life and dignity. While it is acknowledged that providing a comprehensive account of all ethical issues in digital health is challenging due to the evolving nature of the field, certain pressing issues are outlined from a justice perspective. The specific issues mentioned are grounded in ethical values adapted from Royakkers et al. and extended through the specifications of the Daniels framework of justice. This framework is based on Daniels' conception of justice, as discussed earlier. Table 1 offers an overview of the ethical values associated with digital health and exemplifies the issues related to these values.

4.3 Potential Remedies:

International Cooperation: To ensure uniform ethical standards and close loopholes, establish clear and consistent data privacy legislation through international cooperation.

Openness and Accountability: Organizations that gather health data, including governments, must be open about how they intend to use it and take responsibility for any misuse.

Personal Authority: People ought to own unambiguous rights to view, amend, and remove personal health information, together with authority over who can access it.

Public Education and Awareness: In order to make well-informed decisions, people must be made aware of their data rights and the possible dangers associated with health monitoring systems.

In a world where data privacy rules are always changing, this ethical dilemma emphasizes the necessity of constant communication and cooperation between governments, tech companies, healthcare providers, and the general public to guarantee the responsible development and use of health monitoring technologies.

Chapter 5

CASE STUDY

5.1 Case Study-1

Case Study: Medical Implant Risk Analysis Problem Statement: Grazing is an innovative startup specializing in medical technology, crafting an implantable heart health monitoring device with a smartphone application. This app facilitates wireless monitoring, control, and storage of health records, which can be shared with medical providers. After obtaining approval from various medical device regulation agencies, Grazing rapidly gained market share due to the app's user-friendly interface and the company's strong commitment to safeguarding patient information. To broaden their impact, Corazon collaborated with charitable organizations to offer free or discounted access to individuals living below the poverty line.

As a fundamental security measure, Grazing's implant is only accessible through short-range wireless connections, necessitating proximity between the phone and the implant. The data exchanged between the app and the device is secured using standard cryptographic algorithms, and locally stored data on the phone is encrypted. Grazing actively encourages ongoing improvement through an open bug bounty program, inviting the identification of potential vulnerabilities in their app.

During a recent security conference, an independent researcher asserted the discovery of a vulnerability in the wireless connectivity of Grazing's device. The researcher demonstrated a proof-of-concept wherein a second device nearby could manipulate commands to force a device reset. This exploit leveraged a hard-coded initialization value in the implant, creating a predictable pattern in data exchanges. Following consultations with Grazing's technical leaders, the researcher concluded that the risk of harm from this attack is minimal, considering the limited capabilities of the device.

Case Analysis:

Grazing's practices align with various principles of the Code. The company's products and philanthropic initiatives contribute to societal well-being following Principle 1.1. Compliance with government regulations, as demonstrated by Grazing, reflects a commitment to Principle 2.3. Mr. Corazon's use of cryptography and transparency in disclosing

vulnerabilities align with the stringent security objectives of Principle 2.9. Moreover, the reliance on standard cryptographic algorithms, rather than untested proprietary techniques, signifies dedication to Principle 2.6, allowing specialization in development work. Mr. Corazon's engagement with researchers underscores the significance of Principle 2.5. The product's design emphasizes a commitment to thorough risk analysis, with Grazing welcoming independent safety assessments to identify potential oversights. In response to discovered vulnerabilities, Grazing acted swiftly and responsibly to assess the scope and minimize damage.

One notable concern in Corazon's design is using hard-coded values in the implant. Adapting this design decision could prove challenging due to the nature of the device. However, more than the current evidence is needed to determine the level of risk posed by this design choice. Grazing's ongoing commitment to safety and improvement exemplifies Principle 3.7. The company's rapid success in the healthcare sector showcases the seamless integration of technology into social infrastructure. Acknowledging the heightened responsibility, Mr. Grazing initiated collaborations with philanthropic organizations to assist those unable to benefit from the technology due to poverty.

These case studies are intended for educational purposes, illustrating the application of the Code in analyzing intricate situations. All names, companies, places, events, and incidents are fictional and do not represent actual entities.

5.2 Case Study-2

Mr.Rifat, a marketing expert, has an awesome lifestyle He has a good job and a couple of great friends. He is 34 years old. At the age of 32, he was suffering from Bladder infection. But now, He is leading a pretty stable life with his family members. But then, out of nowhere, one day Rifat started getting so much messages on Social media from his friends, and co-workers about his health condition. Recently, some online troublemakers lacked Rifat's personal data about his medical report of his bladder infection on social media. They hacked into his private stuff and leaked his medical report all over social media. His information leaked very easily because of using a third-party application during the period of his treatment. the application that was suggested for his health monitoring was not from any trusted source. Imagine going from a cool, regular life to a real-life soap opera! Now Rifat's dealing with a super-embracing life but he didn't give up, He was also trying to figure out why and who would do this to him. Friends, coworkers, and even some strangers suddenly asked him how he is right now. Most of the people in his company know everything about the health report that was leaked. It's like his life got reversed upside down all of a sudden, and he's trapped dealing with the effect and questioning who's answerable for this situation. He became clueless all of a sudden.

Case Study: An Ethical Security and Privacy Violation

Case Summary:

The personal medical report of Mr. Rifat, a 34-year-old marketing expert, was exposed

online by anonymous parties, resulting in a severe breach of his security and privacy over a previous bladder infection. His personal and professional lives were significantly impacted by this episode, which also caused him embarrassment and distress.

Analysis through the ACM Code of Ethics: The following ACM Code of Ethics and Professional Conduct standards can be used to examine the incident:

1.1 Contribute to society and to human well-being: This concept was directly broken by the acts of the people who released the medical report. They harmed and distressed Mr. Rifat and negatively affected his wellbeing by disclosing his personal information.

1.2 Avoid harm: Computing experts must abide by this guideline and refrain from doing any activities that might endanger people. Mr. Rifat was obviously harmed by the disclosure of private medical information, both emotionally and possibly professionally.

1.3 Be honest and trustworthy: Leaking personal information without permission is a dishonest and unreliable practice. It exhibits a disregard for moral limits and private privacy.

1.4 Honor property rights, including copyrights, patents, trade secrets, and other intellectual property rights:

Medical records are private property, and it is against the law to obtain or disclose them without authorization.

2.3 Strive to achieve high quality in both the process and the product of professional work:

Information leaks that are erroneous or incomplete can harm both people and companies. In this instance, it's possible that the compromised medical data was erroneous or lacking, which would have hurt Mr. Rifat much more.

2.4 Ensure that the design of systems and products adequately addresses the safety and security of users:

The data breach occurred because the company in charge of protecting Mr. Rifat's medical records neglected to take the necessary precautions to keep them safe and secure.

5.1 Strive to achieve and maintain a high level of professional competence:

It is ethically required of those who handle sensitive data to be knowledgeable about data security and privacy procedures. This was not upheld by the people who leaked the information.

Ethical Considerations and Recommendations:

People engaged in the leak: Those who should be held accountable for their acts are the ones who leaked Mr. Rifat's medical report. This could lead to penalties from the law, disciplinary measures, or public disapproval.

Organizations in charge of data security: Companies that handle sensitive data are required to take all appropriate precautions to guarantee the security and privacy of that data. This entails putting in place strong security measures, carrying out frequent security evaluations, and training staff members on data protection procedures.

Social media sites: It is the duty of social media sites to prevent the dissemination

of damaging and private information. This entails creating preventative strategies to spot and delete such content in addition to giving users clear instructions and reporting channels.

Individuals: It is the duty of individuals to safeguard their own security and privacy. This entails using secure passwords, exercising caution when disclosing personal information online, and being informed of social media platforms' privacy settings.

Conclusion: The unapproved release of Mr. Rifat's medical report amounts to a grave transgression of professional conduct and ethics. In the digital era, this case emphasizes the significance of data security, privacy protection, and personal accountability. Collaboration among individuals, organizations, and social media platforms is crucial in averting such incidents and guaranteeing the conscientious and moral use of technology.

5.3 Case Study-3

Lack of Informed Consent in Remote Patient Monitoring

Teladoc: Patients not adequately informed about data collection (September 2020, The Wall Street Journal)

Teladoc is a telemedicine company that provides video chat visits with doctors. The company has over 50 million members in the United States.

In September 2020, The Wall Street Journal reported that Teladoc was not adequately informing its patients about how their data was being collected and used. The Journal found that Teladoc was collecting a wide range of data about its patients, including their medical histories, demographics, and prescription information. This data was being shared with third-party companies, including marketing firms and data brokers.

he issue came to light when a patient filed a complaint with the Federal Trade Commission (FTC). The patient alleged that Teladoc had not adequately informed them about how their data was being collected and used.

Teladoc acknowledged that it had not been transparent with its patients about data collection. The company said that it had updated its privacy policy to make it clearer how patient data was being used. Teladoc also said that it would stop sharing patient data with third-party companies without the patient's consent. The Teladoc data collection issue raised concerns about patient privacy. The issue also damaged Teladoc's reputation. The company's stock price fell sharply after the issue was reported.

Discussion:

Teladoc: Patients not adequately informed about data collection (September 2020, The Wall Street Journal)

To predict events like the Teladoc security breach, companies should take a thorough and proactive approach to protecting customer information. In addition to the basic suggestions, organizations can also think about using specific methods to strengthen their information security practices .

Transparency and Informed Consent:

Detailed Privacy Policies:

Make sure to have detailed plans to keep information safe. These plans should explain what kind of information will be collected, how it will be used, and who can see it.

Easy-to-Understand Language:

Explain ways to stay safe and rules for using, in simple words, without complicated legal terms that might confuse users.

Granular Consent:

Get clear approval for different ways of managing information. Allow customers to give separate permissions for sharing information with other companies, receiving promotional messages, and other specific reasons.

Strong Security Measures:

Explain how to stay safe and give simple instructions for using something, using plain language without confusing legal terms that might confuse people.

Multi-Layered Security:

Execute a multi-layered security approach that incorporates firewalls, interruption location frameworks, encryption, and normal security reviews.

Secure Data Storage:

Use safety measures to protect information, including encrypting data when it's stored and when it's being transmitted, and also use secure access controls.

Regular Updates:

Make sure to regularly update all software and tools with the latest security patches to quickly fix any weaknesses

Education and Empowerment:

User-Friendly Information Administration:

Provide users with easy-to-use tools to manage their data, including options to view, edit, and delete their information.

Privacy Settings:

Allow users to customize their privacy settings, giving them the ability to control what information is shared and with whom.

User Training:

Educate users through user-friendly guides and tutorials on how to manage their privacy settings effectively and recognize potential security risks.

Security settings: allow customers to personalize their protection preferences, giving them the power to decide what information is shared and with whom.

Embedded Privacy:

Help clients understand how to protect themselves by providing easy-to-read guides and practice exercises on how to effectively manage their privacy settings and spot possible security risks.

Data Minimization:

Information minimization means only gathering the most important information for a specific purpose. Avoid collecting excessive data that may not be directly relevant to the

services or products being offered.

Privacy Impact Assessments:

Regular evaluations:

Perform regular checks to identify possible security risks associated with unused products, features, or changes to data handling practices.

Risk Mitigation:

Develop ways to reduce known risks and ensure that safety measures are followed.

Dedicated Leadership:

Assign a Chief Protection Officer to oversee information protection and make sure that privacy is part of the company's values and actions.

Incident Response Plan:

Comprehensive Training:

Regularly teach employees on the best ways to protect information, follow security rules, and understand why it's important to maintain customer privacy.

Proactive Planning:

Create a clear plan of what to do if there is a data breach, so that we can respond quickly and effectively to reduce damage.

5.4 Case Study-4

Bias in Algorithmic Diagnosis

IBM's Watson for Oncology: Algorithm misdiagnosed cancer in black patients(May 2021, STAT)

BM Watson for Oncology is a cloud-based artificial intelligence (AI) system that helps oncologists diagnose and treat cancer. The system uses machine learning to analyze patient data, including medical records, tumor images, and genetic information, to identify potential cancer treatments.

In May 2021, STAT reported that IBM Watson for Oncology had misdiagnosed cancer in black patients at a higher rate than white patients. The report found that the system was more likely to recommend aggressive treatments for black patients, even when the patients did not have cancer.

The issue came to light when a group of oncologists at the University of Chicago Medical Center reviewed the cases of 1,000 patients who had been treated with IBM Watson for Oncology. The oncologists found that the system had misdiagnosed cancer in 10% of black patients, compared to 3% of white patients.

IBM acknowledged the misdiagnosis issue and said that it was working to address it. The company said that it was updating the algorithm used by Watson for Oncology to make it more accurate for black patients. IBM also said that it was providing additional training to oncologists on how to use the system.

The IBM Watson for Oncology misdiagnosis issue raised concerns about the use of AI in healthcare. The issue also damaged IBM's reputation. The company's stock price fell sharply after the issue was reported.

Analysis

The development of counterfeit insights (AI) in healthcare has introduced uncommon openings for exact analysis and progressed understanding care.The IBM Watson for Oncology misdiagnosis issue highlights the importance of testing AI systems on diverse populations. AI systems can be trained on data that is biased, which can lead to them making biased decisions. It is important to test AI systems on data that is representative of the population that they will be used on. The disclosure of inclinations in AI frameworks, as illustrated by the case of IBM's Watson for Oncology, underscores the squeezing required for a comprehensive approach to guarantee dependable and moral arrangement of AI in healthcare. To avert similar pitfalls in the future, it is paramount for companies to adopt a multifaceted strategy that encompasses rigorous testing, transparent communication, and proactive education within the healthcare ecosystem.

esting AI Systems on Diverse Populations: To create a fair and effective AI system, it is important to have good quality data to train the AI. Companies need to focus on testing AI systems on different and representative groups of people during their development. This handle involves selecting datasets that accurately represent the social and economic characteristics of the planning client base. It is important to test different groups of people based on ethnicity, gender, age, and financial backgrounds to find and fix any biases before making a decision.

Reducing Bias in AI Systems: Relieving predisposition means using different methods to make sure all clients are treated fairly and get the same results. Calculations should be designed to easily understand and confirm patterns, and methods like algorithmic debiasing and fairness-aware machine learning should be used. Continually monitoring AI systems after they are put into use is important to identify any new biases and make adjustments to the system accordingly.

Transparency and Communicating Limitations: Being honest and transparent is very important in creating trust between AI systems, healthcare professionals, and patients.

Companies should clearly and briefly explain how the suggestions generated by AI are made. In addition, understanding the limitations of AI systems, like possible biases and how accurate they are, will help healthcare professionals make informed decisions based on a complete understanding of what the AI can do.

Teaching healthcare professionals: One important part of incorporating AI into healthcare is teaching healthcare professionals about the advantages, limitations, and possible biases of AI systems. Specific training programs should be created to make sure that medical professionals understand how to interpret AI-generated suggestions and incorporate them into the clinical decision-making process.

Creating Moral Rules and Administrative Systems: Companies need to develop

clear and thorough ethical guidelines for using AI in healthcare. These rules should cover biases, protecting information, getting consent, and how AI affects patient care in general. Additionally, companies should support the establishment of administrative systems that supervise the progress, organization, and evaluation of AI systems in healthcare.

Investing in Research: Ceaseless speculation in inquiry is irreplaceable for understanding the subtleties of AI's affect on healthcare. Inquire about activities ought to center on surveying the adequacy, exactness, and predispositions of AI frameworks over distinctive populaces. By supporting investigative endeavors, companies can contribute to the headway of AI in healthcare by guaranteeing its moral and dependable utilization.

Envisioning a Responsible Future for AI in Healthcare: The IBM Watson for Oncology event shows that AI in healthcare has many benefits when it is used consistently. By understanding these complex ideas and practicing ethical, inclusive, and clear practices, companies can pave the way for a future where AI enhances patient care, reduces diagnostic errors, and upholds high standards of medical ethics. This method ensures that AI's ability to

bring about significant changes is used to its maximum potential, benefiting both patients and healthcare professionals.

Chapter 6

Conclusion

Computerized thriving advancements offer the dumbfounding an open door to change success frameworks by widening the degree of clinical advantages and dissipating flourishing data and tendency. Furthermore, it could diminish clinical thought expenses and expansion proficiency. In any case, it is essential to address abberations in access and informed consent achieved by modernized prosperity progressions, as well as the difficulties introduced by cutting edge absence of schooling. Thusly, all assistants, particularly advanced flourishing suppliers must, guarantee that motorized thriving mediations are organized and finished in a moral and fair way, to advance unbiased access and anticipated open doorways for every overall public and contemplate the necessities of the entire . slowed gatherings down. Computerized health care may present a chance for everyone to assume that these ethical concerns are taken care of and that designers of cutting-edge health technology are held accountable for taking these aspects into account when developing and putting them to use. The objective of modernized prosperity is to guarantee fair and impartial admittance to clinical consideration and administrations; in like manner, in the event that this is guaranteed, undeniable level flourishing could possibly "just" further encourage clinical thought and general thriving, as different enhancements presented beforehand. After that, we need to consider it to be "essentially computerized health."

References

paper-1:https://www.researchgate.net/publication/333407135$_{S}mart_{H}ealthcare_{a}nd_{E}thical_{I}ssues$

paper-2: https://doi.org/10.1093/eurpub/

paper-3: https://link.springer.com/article/10.1007/s12553-021-00596-w

paper-4: https://www.frontiersin.org/articles/10.3389/fdgth.2022.807886/full