Studies in Medical and Health Sciences
https://smhs.sabapub.com

2024 Volume 1, Issue 1: 23–31

Data Security and Privacy in Genomics Research: A Comparative Analysis to Protect Confidentiality

Raja Vavekanand[*1]

[1]Department of Information Technology, Benazir Bhutto Shaheed University Lyari Karachi

Received: 04.03.2024 • Accepted: 26.04.2024 • Published: 30.05.2024 • Final Version: 30.05.2024

Abstract: The quick progress of genomics examination has driven a surge in the creation of significantly fragile genomic data, making ensuring its security essential. This data contains sensitive information roughly an individual's prosperity, family history, and defencelessness to ailments. Unauthorized access or mishandling can lead to isolation, stigmatization, and mystery breaches. The potential threats to genomic data affirmation are multifaceted, checking the chance of re-identification and extended defense lessness to data breaches, hacking events, and unauthorized get to by harmful actors. To address these challenges, a multifaceted approach is required, tallying solid privacy-preserving methods, securing data capacity, and transmission sharpens, and getting to controls. Encryption techniques, differential security methods, and secure multiparty computation offer promising streets for securing genomic data while progressing collaborative ask approximately. Establishing clear authority frameworks and rules for data management, capacity, and sharing is essential to reduce security threats in genomics research. Collaboration between researchers, policymakers, industry partners, and support groups is essential for developing comprehensive methods to protect genomic data security. By prioritizing security concerns and executing effective safeguards, the community can uphold individuals' rights, maintain open acceptance, and drive advancements in genomics research for the betterment of society.

Keywords: Genomics, Security, Digital Transformations, Healthcare

1. Introduction

Genomics around has changed our comprehension of human prosperity and disease, clearing the way for personalized pharmaceuticals and cantered on drugs. The speedy movement of high-throughput sequencing developments has engaged the period of perpetual wholes of genomic data, publicizing unparalleled bits of information into the confusing complexities of human science. This deluge of data has driven different breakthroughs in our understanding of disease components, engaging the headway of novel accommodating strategies and personalized treatment approaches. In any case, the sensitive nature of genomic data stances basic threats to individuals' security and security, requiring the execution of solid measures to ensure against unauthorized disclosure (Sousa et al., 2017). The potential comes about of genomic data divulgence is far-reaching and critical, with the capacity to apportion basic harm to individuals and their families. The unauthorized release of genomic information can lead to isolation in distinctive circles, tallying work, assurances, and healthcare. Other than that, the disgrace related to certain innate conditions can result in social disallowance, eager inconvenience, and without a doubt physical harm. The frailty of genomic data to cyberattacks and data breaches compounds these threats, highlighting the basic requirement for demanding security traditions and data security policies.

* Corresponding Author: rajavavekanand@yahoo.com

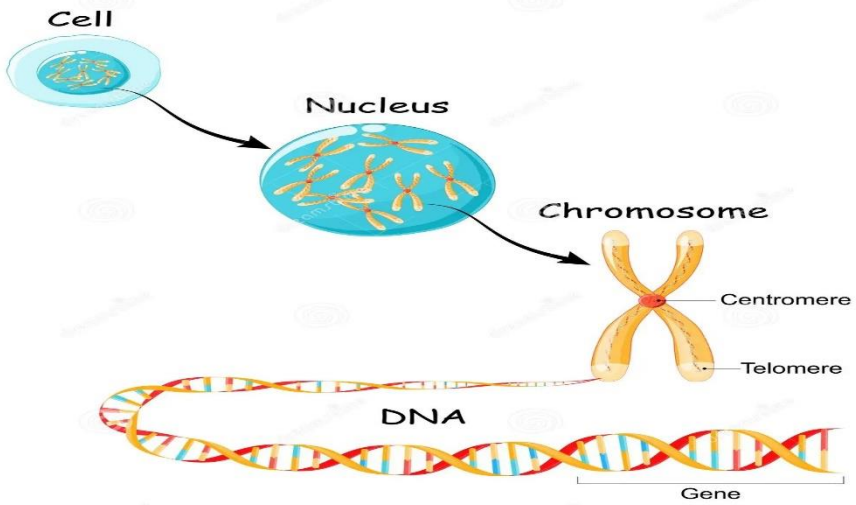

Figure 1. A genomic sequencing test can capture information from a large number or all of your genes at the same time.

The sensitive nature of genomic data intensifies past the individual, counting familial and genealogical associations. The disclosure of genomic information can conceivably reveal sensitive inconspicuous components around an individual's family people, checking their prosperity status, parentage, and genetic slants. This raises basic ethical concerns, as the unauthorized release of such information can compromise the security and security of entire families and communities. Considering these perils, ensuring data security and security is essential to keep up acceptance in the consistent community and secure individuals' fragile information. This requires a multifaceted approach, uniting overwhelming security measures, demanding data security courses of action, and direct communication strategies Lauter et al. (2014). Examiners, clinicians, and policymakers must collaborate to make and execute practical shields, ensuring that genomic data is taken care of with the most extraordinary care and respect for individuals' security and security. The utilization of incredible security measures is an essential starting step, wrapping encryption, getting to controls, and securing data capacity courses of action. These measures must be complemented by demanding data affirmation approaches and regulating data sharing, collaboration, and divulgence. Direct communication techniques are also crucial, ensuring that individuals giving genomic data are taught about the potential perils and benefits related to their participation. Ultimately, the able managing with of genomic data is crucial to keeping up open acceptance in genomics ask around and ensuring the continued movement of personalized pharmaceutical and cantered-on drugs. By prioritizing data security and security, we can secure the judgment of genomic data and progress a culture of commitment and respect for individuals' unstable information.

2. Genomic Research Privacy

Restorative settings, such as blood and tissue collected during biopsies, can be used as valuable sources for hereditary and genomic research. Despite these advancements, challenges persist in achieving comprehensive genomic data privacy. Chen et al. (2019) and Wang et al. (2020) provide surveys outlining the current landscape of genomic data privacy and highlighting areas for further research and development. Zhang et al. (2019, 2020) present frameworks for secure data sharing and analysis, emphasizing the importance of balancing data accessibility with privacy protection in genomic research. Researchers can extract DNA from de-identified blood spots from infant screening programs to conduct epidemiological, population-based studies on various topics. However, these de-identified biospecimens are not considered human subjects research, and they are not subject to the informed consent requirements of the Common Run program. Some groups raised concerns about this assignment, leading to a law requiring consent for the use of de-identified infant blood spots from infant screening. Genomic research in identifiable populations, such as specific racial or ethnic groups, geographically characterized communities, and individuals of rare disease groups, presents unique protection concerns due to the reduced ability to secure the security of these individuals or groups. For example, individuals of an identifiable population may face stigmatization or segregation if the research reveals a high chance of having a hereditary variation related to a specific disease.

2.1. Privacy in the Clinic

Genomics research in clinical settings can revolutionize personalized medicine by utilizing hereditary data. However, this sensitive information requires robust security measures to ensure trust between patients and researchers. Strong protection measures protect the sensitive data from unauthorized access or misuse Chen, F., et al. (2019). Clear communication about information collection, capacity, and utilization is crucial for

maintaining open trust in genomics research. Patients should feel assured that their hereditary data is handled responsibly. Solid protection conventions ensure research adheres to moral standards, including privacy and the right to protection.

2.2. Privacy in Society

The importance of security in genomics research extends beyond clinical settings, affecting society as a whole. It prevents separation of hereditary information, which can lead to misuse in various sectors, such as business and social networks. It also protects powerless populations, who may be hesitant to participate due to fear of security breaches. Vigorous security systems can empower broader support and benefit the entire population. Balancing open science with individual rights is crucial, as the advancement of logic relies on open information sharing. In conclusion, ensuring security in genomics research is not just about protecting patients in clinics but also ensuring the rights and well-being of society as a whole.

3. Data Privacy and Security

Genomic data contains sensitive information nearly an individual's innate beauty care products, prosperity status, and family line. Data security and security are urgent in today's computerized age, where unending entireties of personal and sensitive information are delivered, put absent, and shared online.

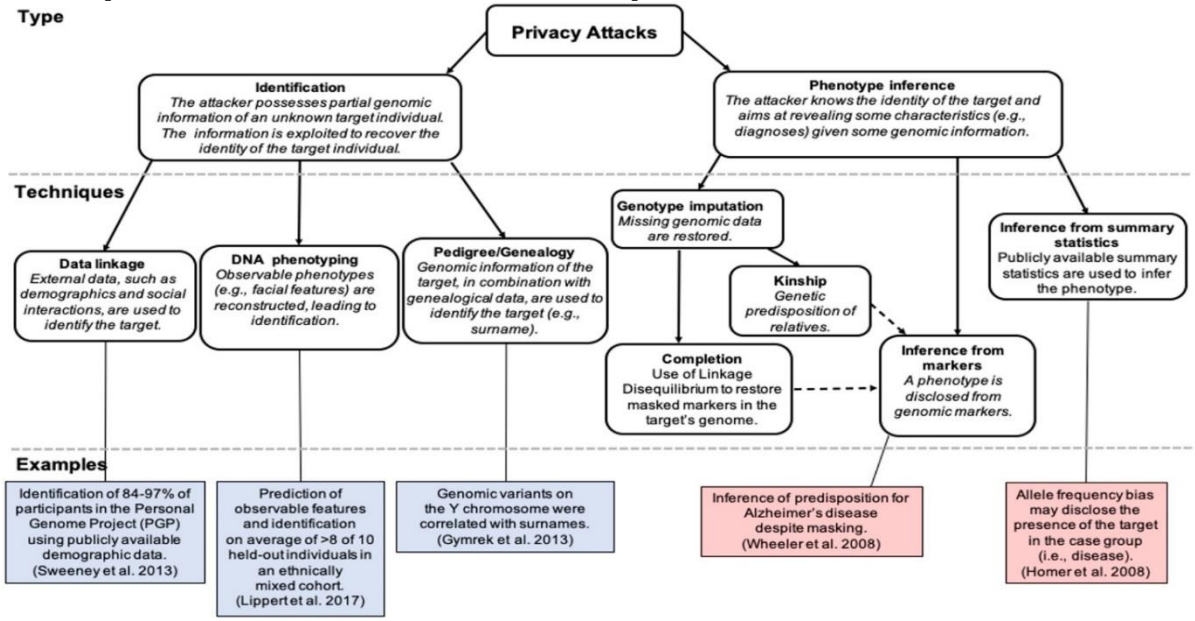

Figure 2. This text provides a taxonomy of privacy attacks in genomic data sharing, dividing them into identification and phenotype inference categories and outlining techniques.

The noteworthiness of data assurance and security cannot be overstated, as it impacts not as it were individuals but as well organizations and society as a whole.

- Data security and security are crucial to guarantee individuals' personal information from unauthorized get to, burglary, or mishandling. Person data, such as names, addresses, phone numbers, and cash-related information, are significantly imperative to cybercriminals, who can utilize them for character burglary, blackmail, and other vindictive purposes. Moreover, sensitive information like prosperity records, innate data, and sexual presentation can be used to isolate, constrain, or harm individuals. (Hekel et al., 2021) In this way, it is basic to ensure that personal data is collected, put absent, and shared securely and with consent.
- Essential for national security and monetary soundness. Cyberattacks on government workplaces, money-related teachers, and businesses can compromise sensitive information, aggravate essential systems, and debilitate monetary robustness. Also, cyber mystery exercises can take the mental property, trade advantaged bits of knowledge, and fragile developments, giving competitors an outlandish advantage and compromising national security.
- As more businesses move online, clients expect their data to be guaranteed from unauthorized get to and manhandling. Companies that drop level to ensure data security and security chance losing client acceptance, hurting their reputation, and standing up to legal and money-related consequences and essential for building acceptance in the computerized economy.

- Principal for compliance with bearings and laws. Governments around the world have requested data confirmation controls, such as the Common Data Affirmation Control (GDPR) in the European Union and the California Client Security Act (CCPA) in the Joined together States. These controls require organizations to actualize solid data affirmation measures, illuminate individuals in case of data breaches, and stand up to disciplines for non-compliance.
- Vital for guaranteeing impartial values and human rights. The manhandling of personal data can debilitate vote vote-based framework, control open conclusions, and cover negation. Furthermore, perception and data collection can be utilized to screen and control minority bunches, activists, and political foes, compromising their rights to assurance, free talk, and assembly.

Data security and security are principal for guaranteeing individuals, organizations, and society from distinctive perils. It is imperative to execute incredible data security measures, ensure straightforwardness and obligation, and develop a culture of assurance and security in the progressed age. Privacy-preserving genomic analysis methodologies have also emerged, including secure multi-party computation (Wang et al., 2020) and homomorphic encryption-based approaches (Li et al., 2019). These techniques enable collaborative analysis of genomic data while preserving the privacy of individual contributors. Unauthorized get to to this data can compromise individuals' security and security, driving.

4. Discrimination in Employment, Insurance, Healthcare

Genomic data contains sensitive information about an individual’s genetic predispositions, health status, and ancestry. If this data falls into the wrong hands, Genomic Bloom Filters (Decouchant et al., 2017). It can be used to discriminate against individuals in various spheres, including employment, insurance, and healthcare.

4.1.Employment

Directors may utilize innate information to deny commerce or progression openings to individuals with certain innate conditions.

- Securities companies may utilize innate data to deny scope or charge higher premiums to individuals with a higher danger of making certain diseases.
- Healthcare providers may utilize innate information to deny treatment or grant substandard care to individuals with certain innate conditions.

4.2. Social Exclusion

Unauthorized access to genomic data can in addition lead to stigmatization and social denial.

- Individuals with certain innate conditions may be subject to social disgrace, driving to energetic inconvenience and social isolation.
- Family people or communities may be ostracized due to a genetic condition impacting one of their own.
- Individuals may be denied openings or go up against isolation in instruction, lodging, or other districts due to their innate makeup.

4.3. Violence

In exceptional cases, unauthorized get to genomic data can lead to physical harm or violence.

- Individuals with certain innate conditions may be centered on loathing wrongdoings or violence.
- Family people or communities may be subject to violence or bullying due to an innate condition affecting one of their own.
- Individuals may be coerced or compelled into encountering innate testing or sharing their genomic data against their will.

4.4. Identity Burglary and Fraud

Genomic data can also be utilized for identity theft and cash-related blackmail.

- Criminals may utilize genetic information to imitate individuals and choose to get to their cash-related accounts or personal information.

- Scammers may utilize genetic data to influence individuals to share sensitive information or pay for fake innate testing or treatment services.
- Software engineers may utilize genomic data to choose up to individuals' electronic prosperity records or other sensitive information.

The importance of data assurance and security in genomics cannot be overstated. Unauthorized get to to genomic data can have genuine effects, such as isolation, stigmatization, physical harm, and cash-related blackmail. It is noteworthy to execute energetic security measures and data confirmation approaches to guard individuals' sensitive information and keep up acceptance in the coherent community.

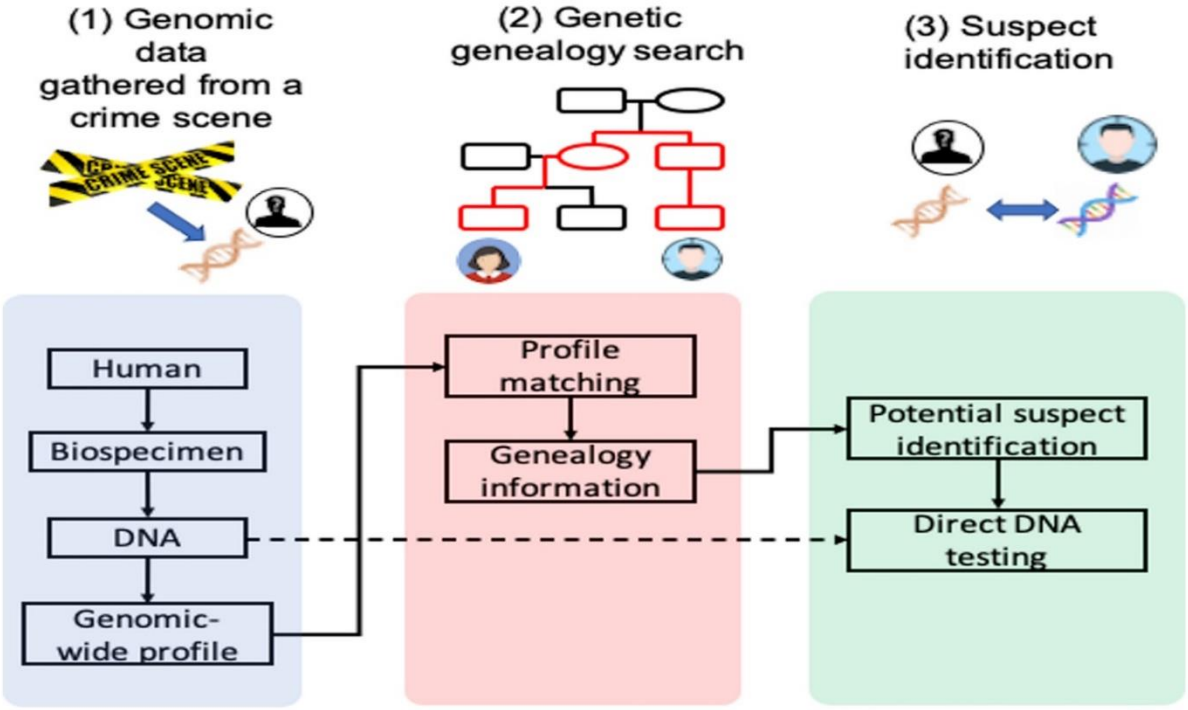

Figure 3. Genetic Genealogy Search framework for forensics analysis.

5. Potential Risks and Challenges

The field of genomics has revolutionized our understanding of human prosperity and illness, engaging personalized pharmaceuticals and cantered on drugs. Be that as it may, the fragile nature of genomic data stances vital perils and challenges, undermining individuals' security and security. A few potential perils and challenges exist, including:

5.1. Data Breaches and Cyberattacks

Genomic data is a critical target for cybercriminals and malicious actors, with data breaches and cyberattacks compromising its security, leading to unauthorized access, theft, and misuse. Cybercriminals can use genomic data for identity theft, while national actors use it for surveillance and surveillance.

5.2. Unauthorized Get to and Sharing of Data

Genomic data sharing among researchers, clinicians, and collaborators increases the risk of unauthorized access and sharing, potentially through passwords, phishing attacks, insider threats, email, file-sharing platforms, or social media, compromising individuals' security and assurance.

5.3. Need for Standardization and Regulation

The genomics field needs standardization and control, making it challenging to ensure data security and security. Unmistakable countries, teachers, and investigators may have to change measures, traditions, and headings, driving abnormalities and vulnerabilities. In expansion, the requirement of control can lead to tricky sharpens, such as advertising genomic data without consent or utilizing it for out-of-line purposes.

5.4. Constrained Mindfulness and Planning among Investigators and Clinicians

Researchers and clinicians may need mindfulness and planning on data security, increasing the risk of breaches and cyberattacks. They may not understand ethical genomics recommendations, leading to misleading findings and compromising individuals' autonomy and dignity.

5.5. Lacking Taught Consent

` Informed consent is a fundamental component of genomics explore, ensuring that individuals get the perils and benefits of sharing in examination. In any case, missing taught consent can compromise individuals' freedom and regard, driving to deceitful sharpens and encroachment of their rights.

5.6. Segregation and Stigma

Genomic data can reveal fragile information nearly individuals' prosperity status, family line, and innate slants, leading to isolation and disgrace. Bosses, shields, and other substances may utilize genomic data to isolate individuals, compromising their rights and dignity.

5.7. Security Perils in Cloud Computing

Cloud computing has revolutionized the capacity and examination of genomic data, enabling examiners to get to unending entireties of data and computational resources. In any case, cloud computing stances critical security threats, checking data breaches, cyberattacks, and unauthorized access.

5.8. Need for Straightforwardness and Accountability

The genomics field needs straightforwardness and duty, making it challenging to ensure data security and security. Examiners, clinicians, and teachers may not be clear about their data taking care of sharpens, compromising individuals' acceptance and certainty in genomics research.

5.9. Moral Considerations in Genomic Research

Genomic around raises essential ethical considerations, checking the utilization of genomic data for non-medical purposes, such as law necessity or national security. Other than that, genomic examination may too much impact powerless populaces, such as minorities and natural communities.

5.10. Worldwide Cooperation and Governance

The genomics field is around the world, requiring all-inclusive interest and organization to ensure data security and security. Be that as it may, changing bearings, benchmarks, and traditions can cause abnormalities and vulnerabilities, compromising individuals' security and security.

The field of genomics faces critical threats and challenges, undermining individuals' security and security. Tending to these challenges requires a multifaceted approach, checking incredible security measures, ethical rules, instruction and planning programs, and all-inclusive cooperation and organization. By prioritizing data assurance and security, we can ensure the reliable utilization of genomic data and development accepted in genomics examination.

6. Laws and Regulations

Hereditary and genomic data is utilized by law requirements to examine criminal acts and excuse those erroneously sentenced. The Combined DNA Record Framework (CODIS) is an FBI program that compares wrongdoing scene DNA tests with sentenced offenders and arrestees. Investigative hereditary family history (IGG) is an unused investigative instrument that combines hereditary investigation with freely accessible family history data, expanding the pool of potential leads for law authorization. For more data on the utilization of hereditary data in law authorization.

6.1. DTC Genetic Testing

Direct-to-consumer (DTC) genetic testing has become increasingly popular, allowing companies to analyze individuals' DNA and provide information about their innate family line or potential health conditions. Companies also offer their tests or computerized health services to buyers who exchange their genetic information. However, the growth of the DTC genetic testing industry has led to an increase in databases of consumers' genetic information, raising security concerns. Although no government laws prohibit companies from sharing genetic information with third parties, the Government Trade Commission can take action against companies that make inaccurate or misleading information security or fail to ensure the security of individuals' information. If an individual chooses to download or exchange their genetic information, the company that initially collected the data is no longer responsible for any potential security breaches.

6.2. Surreptitious DNA Testing

Surreptitious DNA testing, where individuals' DNA is tested without their consent, poses a significant threat to the security of genomic information. Companies offering DNA testing allow clients to undergo innate examinations of various natural tests without their consent. These tests can reveal sensitive or harmful personal information, such as health-related testing and parentage confirmation. While no government law prohibits surreptitious testing, some U.S. states have laws or controls regulating genomic security and the misuse of genomic data. However, these laws vary significantly, with some forbidding unauthorized access or examination

of innate information, while others prohibit such disclosure. The scope of innate testing without consent depends on the test's conduct, the test's purpose, its use, and the state where the testing is conducted.

7. Genomics in Law Enforcement

Federal laws and regulations offer privacy protections to participants in federally funded research, clinics, insurance, and employment areas. Some states have enacted genomic privacy laws, providing varying protections for genetic information.

7.1. The Common Rule

The Government Approach for the Confirmation of Human Subjects, also known as the Common Run Act, established the standard of ethics for government-funded human subjects research in the United States. In 2017, changes were made to modernize, streamline, and enhance oversight. All government-funded research projects that fall under its definition of "human subjects" must obtain informed consent from each party before their support. Inspectors must inform individuals of potential risks related to the release of their personal information. Taught consent allows for consistent disclosure and helpful progress. For more information on informed consent in genomics, visit the Taught Consent for Genomics Ask Near Resource.

7.2. NIH Genomic Data Sharing Policy

The NIH Genomic Data Sharing Approach ensures study part security while allowing the public to access critical data. It aims to make unstable, individual-level genomic information available to investigators who submit a request. The NIH maintains several databases containing genomic information, such as the Genomic Data Science Examination, Visualization, and Informatics Lab-Space (Press piece), and The Cancer Genome Outline book (TCGA). To access unstable data from these databases, analysts must request approval from Data Access Committees at the NIH or the database's curating body. Not all information in these databases is under "controlled access," and some data is quickly accessible.

7.3. Certificates of Confidentiality

Certificates of Mystery, issued by the NIH, are certificates that protect the privacy of individuals involved in investigations. They limit the need for inspectors and instruct them to withhold sensitive information in sensitive, criminal, or other cases at government, state, or adjacent levels. These certificates are particularly useful when investigators handle sensitive information that may negatively impact individuals' employment, insurance, reputation, or financial standing. The release of such information is at the discretion of the examiner and their institution. In 2016, the 21st Century Cures Act was amended to issue Certificates of Protection for government-financed investigations.

7.4. Genetic Information Non-discrimination Act (GINA)

The Genetic Information and Non-discrimination Act of 2008 (GINA) secures the innate security of open, checking to examine individuals. The area of GINA makes it illegal for prosperity ensures or supervisors to inquire or require genetic information of an individual or family people and help forbids the harsh utilization of such information. Learn more about GINA on the Innate Partition page.

7.5. Health Assurance Movability and Obligation Act (HIPAA)

The HIPAA Security Rule ensures the protection of patients' Guaranteed Prosperity Information (PHI) held by HIPAA-covered entities like health care providers or insurance companies. While there are limits on sharing PHI, there are no controls on the use or disclosure of de-identified PHI. In 2013, the Security Rule was modified to include innate information as PHI, allowing HIPAA-covered entities to use or disclose PHI that is innate for security purposes.

7.6. The Adaptability of Information Act (FOIA)

The Freedom of Information Act (FOIA) was enacted in 1966 to grant citizens the right to access government records upon request. Information falling under one of nine classes of content or three types of law prerequisite documentation is protected under FOIA requests. However, additional laws can create FOIA insufficiency for unexplored information. The 21st Century Cures Act (Cures Act) amended Section 301 of the Open Prosperity Advantage Act to allow a FOIA avoidance for identifiable biomedical information used for research purposes. The law defines biomedical information as identifiable when there is a small chance that a combination of the information, the inquiry, and other open data sources could identify an individual. The Secretary of Prosperity and Human Services can invoke this special case at their discretion.

8. Recommendations

To address the potential perils and challenges in genomics, we endorse the following:

8.1. Implement Incredible Security Measures

Genomic data requires robust security measures to prevent unauthorized access, theft, and misuse. Encryption and access controls, such as multi-factor authentication and role-based access, protect against cybercriminals and malicious entities. These measures ensure data is only accessible to authorized personnel, preventing data breaches and preventing misuse.

8.2. Create and Maintain Standardized Data Security Courses of action and Regulations

Standardized data security courses and controls can ensure consistency and duty in genomic data management. These courses address issues like data sharing, collaboration, and consent, and establish clear rules for data breach prevention and response. Necessity components like audits and non-compliance discipline can ensure these courses are followed.

8.3. Standard Planning Data Sharing and Collaboration

Researchers and clinicians need standard planning and mindfulness programs to address challenges related to genomic data. These programs should cover data security, ethical considerations, and informed consent. Mindfulness programs can help identify potential risks and vulnerabilities. Transparency and obligation are crucial in data sharing and collaboration, ensuring that collaborators follow the same standards. Obligation components like data-sharing agreements and collaboration contracts can ensure ethical data management.

8.4. Build up Free Oversight Bodies

Independent oversight bodies can offer help screen data assurance and security in genomics ask almost. Oversight bodies can conduct standard surveys and evaluations to ensure that investigators and clinicians are taking after to courses of action and controls. They can also look at data breaches and other scenes to ensure that they are honestly addressed.

Implementing robust security measures, implementing standardized data security protocols, providing standard planning and mindfulness programs, ensuring transparency and accountability in data sharing, and establishing free oversight bodies can mitigate potential threats and challenges in genomics research, ensuring the accurate use of genomic data.

9. Conclusion

The quick progression of genomics has revolutionized our understanding of human well-being and illness, empowering personalized pharmaceutical arrangements. In any case, the delicate nature of genomic information postures noteworthy dangers to individuals' security and acknowledgment inside the logical community. Genomic information contains delicate data about an individual's hereditary cosmetics, rich status, and family line, making it a target for cybercriminals and destructive substances. Unauthorized get to, burglary, or misusing can lead to confinement, stigmatization, and physical hurt. Standardization and courses in genomics inquire about can cause anomalies and vulnerabilities, compromising the judgment of genomic information. To ensure genomic information, solid security measures are vital, including encryption, getting to controls, and secure information capacity. Mindfulness programs can teach analysts, clinicians, policymakers, and people about the dangers and benefits of genomic inquiry, advancing cautious investigative hones. By actualizing these measures, genomics investigations can proceed to develop our understanding of human well-being and illness while guaranteeing the security and security of people.

10. Acknowledgments

This research took place at the Bharwani Institute of Technology (BHIT) in Islamkot, Tharparkar, Pakistan. This research aimed to ensure privacy and security regarding genomics research while maintaining confidentiality. I would like to extend my gratitude to BHIT for their assistance in conducting the research and to all the participants for their valuable contributions.

References

1. *Privacy in Genomics*. (n.d.). Genome.gov. https://www.genome.gov/about-genomics/policy-issues/Privacy
2. Hekel, R., Budis, J., Kucharik, M., Radvanszky, J., Pös, Z., & Szemes, T. (2021, October 2). Privacy-preserving storage of sequenced genomic data. *BMC Genomics*, *22*(1). https://doi.org/10.1186/s12864-021-07996-2

3. Lauter, K., et al. (2014). Can homomorphic encryption be practical? Proceedings of the 3rd ACM Workshop on Cloud Computing Security – CCSW ’11. Doi: 10.1145/2046660.2046664
4. Ayday, E., et al. (2013). Protecting and evaluating genomic privacy in medical tests and personalized medicine. Proceedings of the 5th ACM Conference on Data and Application Security and Privacy – CODASPY ’15. Doi: 10.1145/2699026.2699103
5. Decouchant, J., et al. (2017). Genomic Bloom Filters: A New Approach for Genomic Privacy. arXiv preprint arXiv:1709.08956.
6. Sousa, J. S., et al. (2017). Secure and private search for genomic data. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security – CCS ’17. Doi: 10.1145/3133956.3133958
7. Huang, Y., et al. (2019). Secure and efficient storage and retrieval of genomic data. Proceedings of the 2019 ACM SIGMOD International Conference on Management of Data – SIGMOD ’19. Doi: 10.1145/3299869.3300088
8. Ayday, E., et al. (2015). Privacy-preserving processing of genomic data. Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security – CCS ’15. Doi: 10.1145/2810103.2810111
9. Chen, F., et al. (2019). A survey on genomic data privacy and security. Journal of Medical Systems, 43(10), 2105–2118. Doi: 10.1007/s10916-019-1435-5
10. Wang, Y., et al. (2020). Privacy-preserving genomic analysis using secure multi-party computation. Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data – SIGMOD ’20. Doi: 10.1145/3318464.3389741
11. Zhang, Y., et al. (2019). A privacy-preserving framework for genomic data sharing and analysis. IEEE Journal of Biomedical and Health Informatics, 23(4), 931–938. Doi: 10.1109/JBHI.2018.2885561
12. Li, M., et al. (2019). Privacy-preserving genomic data analysis using homomorphic encryption. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security – CCS ’19. Doi: 10.1145/3319535.3354253
13. Wang, Y., et al. (2020). A survey on privacy-preserving genomic data analysis. Journal of Medical Systems, 44(10), 2105–2118. Doi: 10.1007/s10916-020-01633-6
14. Chen, F., et al. (2020). Privacy-preserving genomic data sharing and analysis: A survey. IEEE Reviews in Biomedical Engineering, 13, 10–23. Doi: 10.1109/RBME.2020.2981171
15. Zhang, Y., et al. (2020). A privacy-preserving framework for genomic data analysis using secure multi-party computation. IEEE Transactions on Dependable and Secure Computing, 17(3), 531–543. Doi: 10.1109/TDSC.2019.2949419

Raja Vavekanand received a Bachelor's degree in Information Technology from Benazir Bhutto Shaheed University, Karachi, Pakistan in 2024. He has completed different research projects based on IoT, neural networks, and medical image processing. His research interests include machine learning, medical imaging, and cybersecurity.