International Journal of Multidisciplinary Sciences and Arts

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

Data Privacy and Security in Health Informatics: Ethical and Legal Considerations

Mohammed Javeedullah[1*]
[1]New England College 98 Bridge Street, Henniker, NH 03242
[1]JMohammed3_GPS@nec.edu

open access

Corresponding Author

Article History:
Submitted: 15-04-2025
Accepted: 27-04-2025
Published: 03-05-2025

Keywords
Health Informatics, Data Privacy, Data Security, Ethical Principles, Health Data Management, Privacy Risks, Healthcare Technology, Data Protection.

ABSTRACT

Through its approach of digital health data management health informatics has brought extensive transformation to healthcare while delivering improvements to clinical procedures and treatment effectiveness and work processes. Health data management transformation creates substantial privacy and security problems with sensitive health information. This paper examines fundamental health data management problems by analyzing legal standards and security systems together with ethical concepts and innovative technology systems. Health data management practices need to follow ethical principles which include autonomy and beneficence and non-maleficence and justice and these practices must abide by legal frameworks which encompass HIPAA and GDPR. Health data protection requires three essential elements which involve encryption technology with access control systems and audit trail functionality. New privacy along with security challenges emerge from the implementation of block chain and AI and cloud computing technologies which bring opportunities to innovate. This text highlights the requirement for sensible approaches which aim to deliver safe application of technology alongside well-protected information and trusted patient relations and ethical healthcare delivery within advancing digital health settings.

INTRODUCTION

Health informatics bridges healthcare and information technology to facilitate the collection and management of massive health data through storage and data analysis and data sharing purposes in contemporary medicine. Health information creates value in patient care when healthcare providers use electronic health records (EHRs) and mobile health (health) applications together with wearable devices and telemedicine platforms [1]. This information generation supports improved clinical results and administrative efficiencies and research projects and health innovation development. Healthcare digitization introduces new issues regarding patient data privacy and security while generating important benefits from the collection of significant health-related information [2].

Health data presents itself as a main attractor for hackers and unauthorized users due to its highly sensitive nature. Health information differs from financial data since it holds personal medical insights that cannot be replaced regarding a person's physical state and mental condition [3]. Players whose health data is compromised will experience negative effects through identity theft while facing discrimination alongside emotional damage alongside diminished healthcare system trust. Healthcare providers along with policy developers and technology producers face privacy security challenges because health information protection has become their essential focus [4].

The protection of health informatics data needs thorough review of ethical guidelines alongside complete adherence to existing legal mandates. Healthcare professionals should adopt ethical codes that defend patient self-determination together with obtaining informed permissions from patients and minimizing safety risks. Patients need to feel assured their information receives ethical and clear-handled treatment benefiting them directly [5]. Data protection standards emerge from multiple regulations including the Health Insurance Portability and Accountability Act (HIPAA) in the United States together with the General Data Protection Regulation (GDPR) in Europe through which legal standards are created for data collection and storage as well as sharing and protection. The process of handling these regulations continues to create difficulties especially when working across different borders and with digital health practices [6].

The analysis investigates various aspects of health informatics data protection and security throughout a legal and ethical framework. This analysis examines health data varieties along with their security threats while discussing regulatory practices and moral dimensions before investigating novel technological solutions which produce new security concerns. The article examines current practices while defining respective weaknesses to determine responsible health informatics developments for data-oriented environments [7].

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

BACKGROUND ON HEALTH DATA IN INFORMATICS

Health informatics functions on its core principle of managing data collection and management and analysis to benefit healthcare delivery and policy analysis and research. Knowledge about health data basics including its origination points enables complete comprehension of privacy and security requirements [8]. Throughout the healthcare field individuals' health information consists of various data points that cover medical records and testing outcomes and therapeutic strategies as well as their prescribed treatments and their daily activities. The various types of health data can be lab results with structured format or clinical notes with semi-structured organization or unstructured data such as medical images and voice recordings [9].

The base dataset for health information comes from the Electronic Health Record which presents a digital version of patient medical records operated by healthcare providers. Healthcare providers benefit from patient care revolution through EHRs because this system provides better information accessibility as well as enhanced inter professional relationships. The collection of health data also depends on two main components: Personal Health Records managed by patients and mHealth applications utilizing smartphone and wearable technology [10]. Healthcare technologies that include telemedicine platforms and remote monitoring systems and clinical decision support tools develop copious amounts of current healthcare data.

Through health data utilization the sector supports population health management functions as well as medical research operations and public health surveillance while serving health economic activities. Health informatics shifted from basic medical documentation to predictive analytics and customized treatment approaches and system-driven healthcare decisions because of artificial intelligence and big data analytics technology development. This rising complexity combined with bigger data sizes requires strategic security frameworks to become an utmost necessity [11].

The strict nature of protecting health information presents strong obstacles in defense strategies. Personal health information differs from other forms of data because it maintains direct privacy value to patients through identifying characteristics such as full names with residence information and biological data together with insurance-related details [12]. Health information used by informatics systems generates valuable information about patient conduct and how they live their lives while simultaneously exposing their genetic risk factors. The disclosure or unauthorized modification or misuse of these health data points results in patient breaches of trust and legal repercussions together with patient harm. The background context of health data in informatics creates a dual responsibility to pursue data's healthcare improvement potential and systematically protect it from potential threats. Health informatics requires maintaining balance because ethical and legal aspects form the foundation for its responsible practice [13].

ETHICAL PRINCIPLES IN HEALTH DATA MANAGEMENT

Health data management in healthcare requires ethical principles to direct the collection and storage of data and the distribution of information and its utilization. Data protection needs both technical security methods and ethical guidelines to ensure freedom of individual rights and national values are safeguarded. The management of health data in informatics needs to comply with the four basic bioethical principles including autonomy alongside beneficence and non-maleficence together with justice [14].

Patients have the right to determine decisions regarding their medical information after receiving comprehensive information. Health informatics practitioners must guarantee patients receive full information about what data is collected as well as how it will be utilized and who holds access to it. The informed consent process needs to provide meaning to patients through transparent explanations which should never reduce to electronic consent forms [15]. The collapse of autonomy occurs when patients remain in the dark about where their data transfer routes or its secondary utilization for research or business interests.

Health data must serve the dual purposes of promoting individual well-being and avoiding any potential harm through beneficence and non-maleficence. Data analytics, artificial intelligence and health monitoring technologies enhance medical care but healthcare providers need to prevent patients from receiving any new threats through the implementation of these systems including inaccurate diagnoses caused by biased algorithms or emotional distress from unauthorized data sharing [16]. Healthcare providers and developers stand responsible for developing systems that demonstrate both evidence-base work and guarantee fairness while maintaining safety standards.

International Journal of Multidisciplinary Sciences and Arts
E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

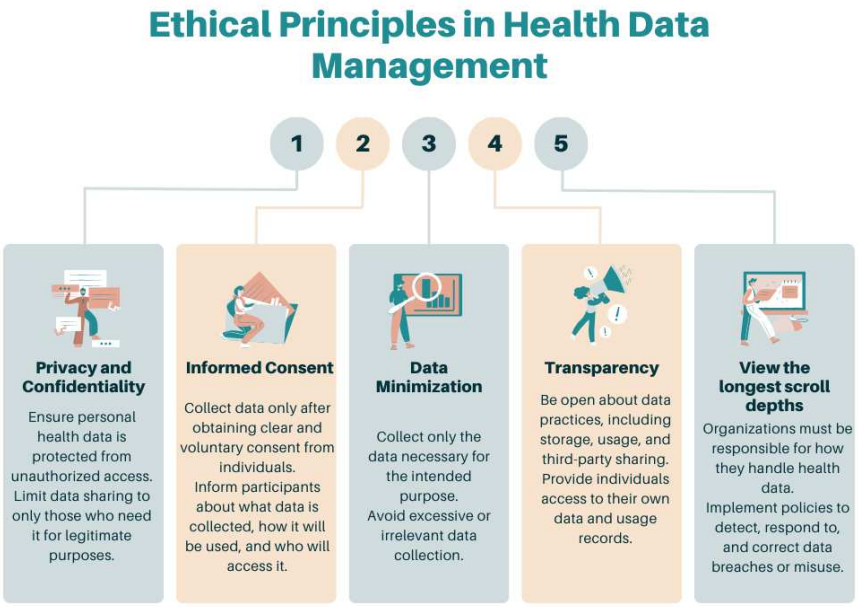

Figure: 1 showing ethical principles in health data management

Justice in health data management pertains to fairness in both data access and outcomes. Ethical data practice addresses discrimination by placing strict measures that prohibit unfair treatment of vulnerable groups including older adults and persons with disabilities while working in disadvantaged areas. People need transparent policies coupled with equal digital tool availability to preserve trust in health informatics systems [17].

Issues with ethical nature commonly emerge when opposing values clash as demonstrated through the case of public health surveillance systems that invade personal privacy. A systematic approach that considers the present situation must be used in these cases. Ethical health data management operates as a living process that shifts based on the development of technology combined with changes in societal standards and patient demands [19].

LEGAL AND REGULATORY FRAMEWORKS

The functional operation of healthcare information relies upon legal structures because these bodies protect medical data through their frameworks that maintain privacy requirements and security standards together with ethical legal standards. Health informatics systems gain their legal protection abilities for patient rights while creating data handler responsibilities through these regulatory statutes. Multiple challenges hinder the effective implementation of diverse health-related laws because they operate across different jurisdictions [20].

The most outstanding legal framework in the United States operates under the Health Insurance Portability and Accountability Act (HIPAA). Healthcare organizations across the nation follow HIPAA standards which were introduced through legislation in 1996 for protecting delicate patient health records [21]. The law requires organizations including healthcare providers and their insurance counterparts along with business associates to deploy security protocols through administrative and technical methods and physical protections for health data privacy. All patients earn the entitlement to view their healthcare records and obtain breach notification through this legislation [22].

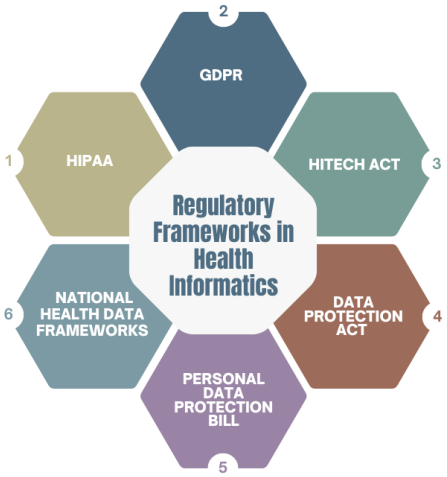

Figure: 2 showing regulatory frameworks in health informatics

International Journal of Multidisciplinary Sciences and Arts
E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

The General Data Protection Regulation (GDPR) under the European Union establishes a complete data protection system which surpasses other existing laws within its domain. The General Data Protection Regulation implements worldwide standards that control all personal data dealing entities starting from 2018 and extends these rules to healthcare facilities along with other organizations [23]. User consent takes center stage while data minimization combines with transparency and allows people to request the deletion of their data. GDPR demonstrates extensive international authority that leads global health platforms to adopt its data policies as a standard model [24]. International data protection appears through two regulatory frameworks where PIPEDA regulates Canada and Digital Personal Data Protection Act enforces India. Legislation in this domain displays three essential differences relating to their role definition and monitoring capabilities and input restrictions [25].

All these legal instruments face difficulties in adapting to changes occurring quickly in AI technology and AI cloud systems and international data sharing systems. The absence of proper regulation and overlapping governance and insufficient monitoring abilities create opportunities for privacy infringements along with misuse cases [26]. The continuous evaluation of legal compliance depends on international partnership together with changes to governing policies and ethical framework alignment to support current laws.

THREATS TO HEALTH DATA PRIVACY AND SECURITY

The digitization of healthcare data together with rising system interconnectivity has led to sophisticated threats against health data privacy as well as security which affect patients on a global scale. Sensitive health information now represents the most lucrative target category for both cybercriminals along with malicious actors [27]. Healthcare institutions face multiple types of severe consequences following health informatics system breaches that harm both individual participants and cost the organization money while damaging its reputation and attracting legal penalties [28].

The leading danger in the current environment includes data breaches that result from cyber-attacks including ransom ware and phishing and malware intrusions. Healthcare organizations generally lack proper cybersecurity readiness due to insufficient resources and this leads them to remain exposed to attacks [29]. The encryption capabilities of ransom ware attacks lead to complete hospital system lockdowns which results in service disruptions and jeopardizes patient health care. Such attacks demand payments from healthcare institutions before releasing access [30].

The organizational system falls under great danger from internal threat actors. Employee mishandling of access privileges becomes a threat when staff members either misuse their privileges on purpose or accidentally create security issues by mistaking harmful links and insufficient data management. Health IT environments now have intricate systems that create total control challenges for managing all available access points [31].

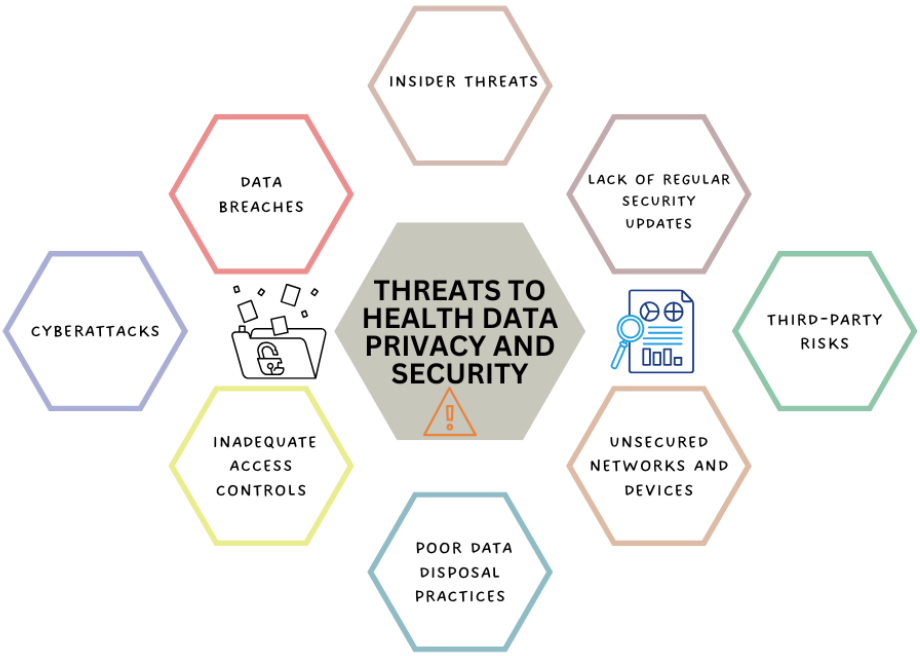

Figure: 3 showing threats to health data privacy security

The danger related to third-party vendors and cloud-based systems operating as health data managers presents a major concern for security. Security vulnerability exists when external partners who handle data have inadequate protection against cyber-attacks. Mobile health application and wearable device data remains vulnerable to exposure because they generally operate outside HIPAA regulatory coverage [32].

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

The process of making data anonymous for research and analytics purposes turns out to be susceptible to reverse identification through data-mining approaches which harms privacy unexpectedly. Additional risks emerge from combining diverse healthcare databases from multiple sources. Health informatics deals with numerous complex threats which continue to change in their nature [33]. Digital security and privacy over sensitive patient information can be achieved through technological protection along with staff training that must follow regulatory guidelines and active management of risks to effectively defend systems.

Security Measures and Best Practices

Information security approaches as well as best practices must be built into health informatics systems to defend sensitive health data from breaches and unauthorized access and misuse. Protecting patient information requires health informatics systems to adopt combined technological methods with administrative and procedural safeguards to guarantee confidentiality and preserve information integrity and ensure availability [34].

Security starts with encryption since it enables safe storage as well as transmission of information. The process of converting sensitive information through encryption makes data impossible to read unless protected decryption keys are available which effectively reduces exposure risks even when systems become compromised. Network-by-network and storage-to-provider transfers of data need this measure as an essential protection [35].

The practice of access control requires authentication methods which include usernames and passwords as well as biometrics and multi-factor authentication (MFA) for limiting data access to authorized personnel. Security benefits from Role-based access control (RBAC) because this method restricts user permissions to the data which corresponds to their work responsibilities thus helping prevent internal security incidents [36].

Medical institutions use data anonymization and de-identification methods primarily for research and analytics purposes as they protect patient identity information. Currently there exists a possibility for re-identification yet security measures need to be handled with proper caution. Anonymization when coupled with encryption provides organizations with superior protection of patient privacy [37]. The combination of audit trails with real-time tracking features enables health organizations to both monitor staff data access and spot any dangerous actions. The monitoring system through software will notify administrators regarding unusual login activity and large data export operations and unauthorized access efforts to enable prompt attention to detected threats [38].

All personnel must receive continuous security training because it constitutes an essential defense measure. Human error remains the cause of most data breaches because staff member action or inaction leads to clicking on phishing links and non-compliance with data-handling guidelines. A workforce equipped with complete knowledge functions as primary defense for the organization. A complete data governance policy keeps both the management and protection methods and storage methods consistent [39]. The organization performs scheduled security evaluation tests and system maintenance procedures alongside authorized implementation of international security protocols including ISO/IEC 27001. A combination of multilayered security practices in healthcare enables organizations to lower their risk exposure so patients maintain trust in digital health services [40].

EMERGING TECHNOLOGIES AND THEIR IMPACT

The fast-paced development of new technologies alters health informatics through both improved healthcare capabilities and heightened risks that endanger patient privacy and security conditions. Technology solutions starting with block chain and artificial intelligence (AI) demonstrate potential and capability in enhancing medical care and optimizing workflow processes and providing tailored medical services [41]. Health informatics tools come with distinct issues pertaining to protecting data as well as ensuring proper ethical conduct.

Healthcare data security finds its most promising solution through block chain technology. Through its decentralized ledger system Block chain establishes secure storage of health data that stays permanent while being impervious to any unauthorized changes. The cryptographic secure methods implemented by block chain systems allow doctors to verify medical records and financial transactions thus protecting such information from unauthorized alterations [42]. Through block chain technology patients achieve improved data control because they maintain complete control over whom can access their information while having strong security for these permissions.

The healthcare sector implements Artificial Intelligence (AI) and Machine Learning (ML) for three primary purposes including data analysis through predictive analytics and decision-making purposes. The healthcare field can use AI to make clinical diagnoses as well as automate administrative work and develop precise treatment solutions using collected patient information [43]. The implementation of AI systems generates privacy-related issues because large medical datasets undergo collection and processing operations. The wide accessibility of health information by algorithms to operate effectively forces healthcare providers to ensure both privacy protection and DE selective AI mechanisms [44].

International Journal of
Multidisciplinary Sciences and Arts

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

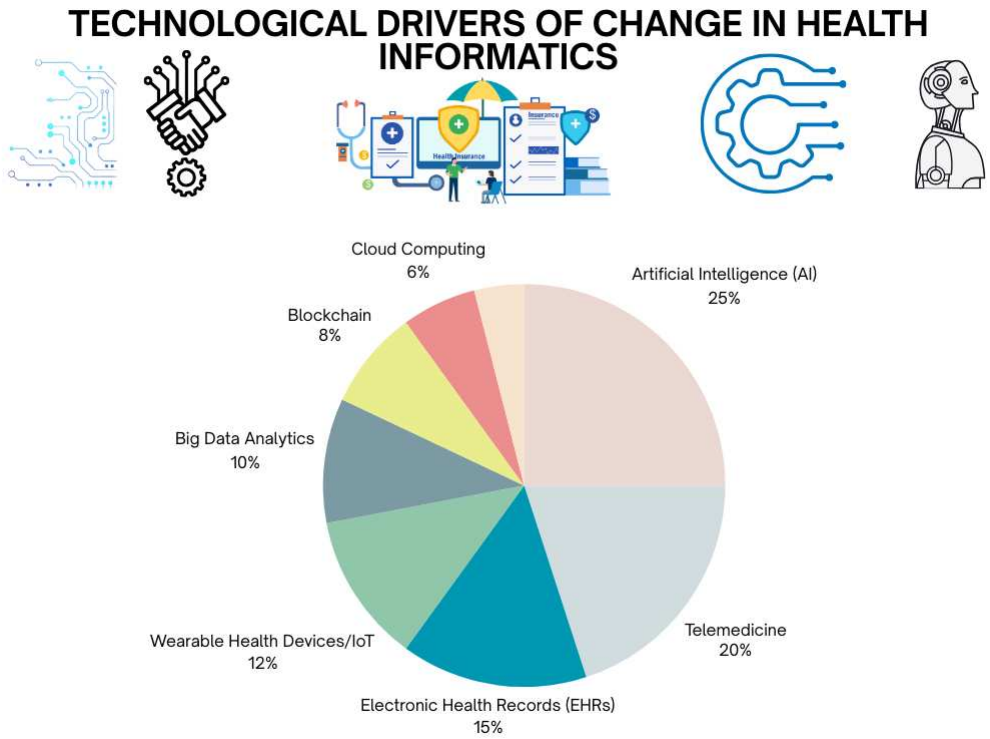

Figure: 4 showing technological divers of change in health informatics

Cloud computing presents an emerging technology that enables organizations in healthcare to work with remote data management services. Cloud systems deliver scalability with flexible power as well as cost efficiency but they present substantial dangers regarding data positioning together with border data movements and vendor security risks [45]. Healthcare providers who use the cloud face complicated problems when they need to maintain security standards while following regulations between diverse international jurisdictions. The implementation of emerging technologies for healthcare purposes requires careful management to protect privacy and security even though they offer great potential for enhanced quality and accessibility together with higher efficiency [46]. Healthcare innovation needs balanced management because it must provide benefits to the healthcare industry without jeopardizing either data security or ethical codes.

CONCLUSION

The growing dependence of healthcare on digital technologies with health informatics forces organizations to put focus on protecting sensitive health data with greater urgency. Patients experience improved health results and coordinated care and health professionals perform clinical tasks better because of digital healthcare system transformations that use EHRs and mobile health applications. Modern digital advance introduces substantial security challenges that stem from cyber-attacks coupled with insider breaches and unauthorized data entry actions.

The management of health data requires health organizations to implement ethical principles including autonomy as well as beneficence non-maleficence and justice. An ethical data management system requires the protection of patient rights in consent decisions along with safe practice standards and equal access to healthcare information. Healthcare institutions face barriers to protect patient data across borders because HIPAA and GDPR present difficulties when implementing legal standards for emerging technologies and international information exchange.

Health data protection depends on implementing encryption and access control and data anonymization and audit trails and staff information security training which together establish robust protection among security measures. New technologies including block chain, AI and cloud computing have both advantages and risks in the healthcare information system. These promising healthcare innovations create fresh security and privacy complexities that healthcare practitioners need to monitor continuously while developing new standard practices. The future success of health informatics will succeed only when medical technology applications do not overshoot their ability to defend patient privacy and secure patient data. The development of ethical and secure and patient-centered Health informatics depends on collaborations between healthcare provider's policymakers together with technologists to protect both technological potential and patient trust in healthcare systems.

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

REFERENCES

[1]. Samuel HW, Zaïane OR. A Repository of Codes of Ethics and Technical Standards in Health Informatics. Online J Public Health Inform. 2014; 6(2): e189. [Cited 2016 August 22]; Available from: URL: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4235322/
[2]. American Health Information Management Association (AHIMA). Code of Ethics. 2006. Revised & adopted by AHIMA House of Delegates – (October 2, 2011). [Cited 2016 August 22]; Available from: URL: http://bok.ahima.org/doc?oid=105098#.V8U1nL55LRq.
[3]. American Medical Informatics Association (AMIA). A Code of Professional Ethical Conduct. 2007. [cited 2016 August 22]; Available from: URL: https://www.amia.org/about-amia/ethics
[4]. Beauchamp, T. L., and Childress, J. F. Principles of biomedical ethics. 6th edition. Oxford University Press, 2009. 2. Layman, E. Health informatics, ethical issues. Health Care Manager. 2003. 22, 1, 2-15.
[5]. Layman. 4. Sittig, D. F. and Singh, H. Legal, ethical, and financial dilemmas in electronic health record adoption and use. Pediatrics. 2011. 127, 4, e1042-e1047.
[6]. Burke W, Pinsky LE, Press NA. Categorizing genetic tests to identify their ethical, legal, and social implications. Am J Med Genet 2001; 106:233–40?
[7]. Fost N. Ethical implications of screening asymptomatic individuals. FASEB J 1992;6:2813–17. 49 Fost N. Ethical issues in genetics. Pediatr Clin North Am 1992; 39:79–89.
[8]. Rogowski WH, Grosse SD, John J, et al. Points to consider in assessing and appraising predictive genetic tests. J Commun Genet 2010; 1:185–94.
[9]. Heshka JT, Palleschi C, Howley H, et al. A systematic review of perceived risks, psychological and behavioral impacts of genetic testing. Genet Med 2008; 10:19–32.
[10]. Rothstein MA. Genetic exceptionalism and legislative pragmatism. J Law Med Ethics 2007; 35(2 Suppl):59–65
[11]. McGuire AL, Fisher R, Cusenza P, et al. Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. Genet Med 2008; 10:495–9.
[12]. Green MJ, Botkin JR. "Genetic exceptionalism" in medicine: clarifying the differences between genetic and nongenetic tests. Ann Intern Med 2003; 138:571–5.
[13]. Gaissmaier W, Gigerenzer G. Statistical illiteracy undermines informed shared decision making. Zeitschrift fur Evidenz, Fortbildung und Qualitat im Gesundheitswesen 2008; 102:411–13.
[14]. Geneviève LD, Martani A, Wangmo T, Paolotti D, Koppeschaar C, Kjelsø C, et al. Participatory Disease Surveillance Systems: Ethical Framework. J Med Internet Res 2019; 21(5):e12273.
[15]. Kalkman S, Mostert M, Gerlinger C, van Delden JJM, van Thiel GJMW. Responsible data sharing in international health research: a systematic review of principles and norms. BMC Med Ethics 2019; 20(1):21.
[16]. J. Mikael Eklund, Thomas Riisgaard Hansen, Jonathan Sprinkle and Shankar Sastry, Information Technology for Assisted Living at Home: building a wireless infrastructure for assisted living, EMBC 2005, Shanghai China, September, 2005.
[17]. M. Evered, S. Bogeholz, a Case Study in Access Control Requirements for a Health Information System, Australasian Information Security Workshop, 2004.
[18]. C. Karlof, N. Sastry, and D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks, Conference on Embedded Networked Sensor Systems, 2004).
[19]. D. Masys, D. Baker, A. Butros , K.E. Cowles, Giving patients access to their medical records via the internet: the PCASSO experience, Journal of American Medical Informatics Association, 2002 Mar-Apr; 9(2):181-91.
[20]. Mascalzoni D, Bentzen HB, Budin-Ljøsne I, Bygrave LA, Bell J, Dove ES, et al. Are Requirements to Deposit Data in Research Repositories Compatible with the European Union's General Data Protection Regulation? Ann Intern Med 2019; 170(5):332-4
[21]. Krutzinna J, Taddeo M, Floridi L. Enabling Posthumous Medical Data Donation: An Appeal for the Ethical Utilisation of Personal Health Data. Sci Eng Ethics 2019; 25(5):1357-87.
[22]. Parasidis E, Pike E, McGraw D. A Belmont Report for Health Data. N Engl J Med 2019; 380(16):1493-5.
[23]. Chevrier R, Foufi V, Gaudet-Blavignac C, Robert A, Lovis C. Use and Understanding of Anonymization and De-Identification in the Biomedical Literature: Scoping Review. J Med Internet Res 2019; 21(5):e13484.
[24]. Erickson BJ, Langer S, Nagy P. The role of open-source software in innovation and standardization in radiology. J Am Coll Radiol 2005 Nov; 2(11):927–931.
[25]. Kobayashi S, Yahata K, Goudge M, Okada M, Nakahara T, Ishihara K. Open source software in medicine and its implementation in Japan. Journal on Information Technology in Healthcare 2009;7(2):95–101.
[26]. Chignard S. A brief history of Open Data [Internet] 2013. Available from: http://parisinnovationreview.com/articles-en/a-brief-history-of-open-data
[27]. Public views on open data. 2013 [cited 2018 Mar 14];(June). Available from: https://forum.kodujdlapolski.pl/uploads/default/original/2X/d/df977225a37ba192982cf408c08926572af775fpdf

E-ISSN : 2962-1658
Volume 4, Number 1 , January 2025
https://doi.org/10.47709/ijmdsa.v4i1.5777

[28]. Obama B. Transparency and Open Government [Internet] 2009 [cited 2017 Mar 30]. Available from: https://obamawhitehouse.archives.gov/thepress-office/transparency-and-opengovernment
[29]. Schairer CE, Cheung C, Kseniya Rubanovich C, Cho M, Cranor LF, Bloss CS. Disposition toward privacy and information disclosure in the context of emerging health technologies. J Am Med Inform Assoc 2019; 26(7):610-9
[30]. Bentzen HB, Høstmælingen N. Balancing Protection and Free Movement of Personal Data: The New European Union General Data Protection Regulation. Ann Intern Med 2019; 170(5):335-7.
[31]. Oxman AD, Paulsen EJ. Who can you trust? A review of free online sources of "trustworthy" information about treatment effects for patients and the public. BMC Med Inform Decis Mak 2019; 19(1):35.
[32]. Chiauzzi E, Wicks P. Digital Trespass: Ethical and Terms-of-Use Violations by Researchers Accessing Data from an Online Patient Community. J Med Internet Res 2019; 21(2):e11985
[33]. Gigerenzer G, Gaissmaier W, Kurz-Milcke E, et al. Helping doctors and patients make sense of health statistics. Psychol Sci Public Interest 2007; 8:53–96.
[34]. Jing X, Kay S, Marley T, et al. Incorporating personalized gene sequence variants, molecular genetics knowledge, and health knowledge into an EHR prototype based on the Continuity of Care Record standard. J Biomed Inform 2012; 45:82–92.
[35]. Green MJ, McInerney AM, Biesecker BB, et al. Education about genetic testing for breast cancer susceptibility: patient preferences for a computer program or genetic counselor. Am J Med Genet 2001; 103:24–31?
[36]. Green MJ, Fost N. An interactive computer program for educating and counseling patients about genetic susceptibility to breast cancer. J Cancer Educ 1997; 12:204–8.
[37]. Green MJ, Biesecker BB, McInerney AM, et al. An interactive computer program can effectively educate patients about genetic testing for breast cancer susceptibility. Am J Med Genet 2001; 103:16–23.
[38]. Green ED, Guyer MS. Charting a course for genomic medicine from base pairs to bedside. Nature 2011; 470:204–13.
[39]. Welch BM, Kawamoto K. Clinical decision support for genetically guided personalized medicine: a systematic review. J Am Med Inform Assoc 2013; 20:388–400.
[40]. Green MJ, Fost N. Who should provide genetic education prior to gene testing? Computers and other methods for improving patient understanding. Genet Test 1997; 1:131–6
[41]. Garg AX, Adhikari NK, McDonald H, et al. Effects of computerized clinical decision support systems on practitioner performance and patient outcomes: a systematic review. JAMA 2005; 293:1223–38.
[42]. Emery J, Morris H, Goodchild R, et al. The GRAIDS Trial: a cluster randomised controlled trial of computer decision support for the management of familial cancer risk in primary care. Br J Cancer 2007; 97:486–93.
[43]. Bernat, J. L. Ethical and quality pitfalls in electronic health records. Neurology. 2013. 80, 1057-1061.
[44]. Weis, J. M. and Levy, P. C. Copy, paste, and cloned notes in electronic health records: Prevalence, benefits, risks, and best practice recommendations. Chest. 2014. 145, 3, 632-638
[45]. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series No. 108. Strassbourg; 28.01.1981. [Cited 2016 August 22]; Available from: URL:https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37
[46]. European Parliament, European Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 October 1995. [Cited 2016 August 22]; Available from: URL: http://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:31995L0046.