

International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307 doi : https://doi.org/10.32628/CSEIT19522101

# Data Privacy and Ethics in Occupational Health and Screening Systems

Yogesh Gadhiya Independent Researcher, USA

#### ABSTRACT

This report describes data privacy and ethics issues in occupational health and screening systems, the challenges and solutions concerning the protection of sensitive employee health information. And as digital health records and workplace monitoring systems grow more widely used, there is an increasing need to guarantee HIPAA and GDPR compliance. The paper examines the role of informed consent, data access control and the ethical implications, specifically in regards to its inclusion of AI and ML integration. The paper highlights the requirements for preparing for the protection of employee's privacy with robust frameworks for efficient health monitoring while ensuring employee trust inside and outside the workplace.

Keywords : Data Privacy, Ethics, Occupational Health, HIPAA/GDPR Compliance

#### Introduction

Increased reliance on digital health records and workplace health monitoring systems has raised major concerns in regards to data privacy and ethics, especially in occupational and screening; however, there has been little research in this regard. Greatest concern has to be the use of employees' sensitive health information in a way that protects employees' privacy and uses the information in an ethical and lawful way. As these systems become more reliant on AI, ML, and IoT, we see that the issues with informed consent, data access control, and those around HIPPA and GDPR are getting more complicated. The stress on occupational health systems in regard to the integration of data privacy, ethics and security is explored boundaryingly, highlighting the importance for strong and solid frameworks to secure health data in workplaces whilst also building trust and compliance in such environment.

#### Literature review

### Data Privacy and Ethics in Occupational Health and Screening Systems

According to Fernández-Alemán et al., 2013. Digital health records and workplace health monitoring systems come under greater reliance, which has raised the prominent issues of data privacy and ethical issues around occupational health and screening in particular. Its big issue is protecting employees' sensitive health information without limiting its use. At the intersection of privacy, security, and ethics, organisational processes of regulation, data access control, and informed consent in occupational health systems are where very careful attention needs to be paid. (Fernández-Alemán et al., 2013). Two major concerned health data protection frameworks in the U.S. are the Health Insurance Portability and Accountability Act (HIPAA) and in Europe the European General Data Protection Regulation (GDPR). In addition, these regulations would impact on occupational health settings in which data on worker health is routinely routinely

collected for worker safety, compliance or performance monitoring purposes. That's why these systems should be run by them to protect against misuse of or unauthorised access to data in strict privacy standards. There's moral issues around how you store and how you access your data and with informed consent. How the data from employees is used, to whom it is accessible, and what effect the health screenings have on employees — all need to be explained to employees.



**Figure 1** : Decurity and privacy in EHR systems (Figure: Fernández-Alemán et al., 2013)

Role Based Access Control (RBAC) is used in many occupational health systems to regulate who should see or change a health record. This model is needed greatly to protect those with specific data from other than those who should have access to it; allowing the occupational health providers or HR departments to have it for proper care and intervention while also protecting privacy. Furthermore, there is increasing awareness that workers in occupational health settings require additional training in security and privacy practises. Today, research shows that there are a number of organisations that fail to teach staff the right ways to handle sensitive data thereby causing inadvertent breaches of privacy. The health screening to maintain workplace safety and respect the employees' privacy are still a very delicate issue ethically. Then new technology in workplace health monitoring becomes better then a promise to adhere to those principles of privacy, informed consent, and strict ethical guidelines absolutely protecting employee trust and well being is needed.



Figure 2 : PRISMA flow diagram(Figure: Fernández-Alemán et al., 2013)Data Privacy and Ethical Considerations

# Occupational Health and Screening Systems

According to Smith et al., 2011. As digital occupational health record and screening systems accumulate more and more sensitive employee health data, the data privacy and ethics in occupational health and screening systems have become an important area of research. The increasing popularity of workplace health monitoring and screening programmes raises new issues of who owns and controls the data, and how any associated information is used. Concerns about employee health information protection been have noted in information privacy research as a call for robust frameworks to secure both employee health information needs with workplace safety and

in

regulatory compliance requirements. There have been a number of studies emphasising the importance of clear conceptualizations of privacy in particular with respect to what qualifies as private health data and who should be responsible for handling it employers or third parties — because of its relationship with informational privacy (Nielsen *et al.*, 2010). The main focus of ethical issues related to occupational health systems is on the informed consent, on data ownership and on the transparency of the data use.



**Figure 3** : Approaches to Defining General Privacy (Source: Smith *et al.*, 2011)

All employees must know how their data will be used, by whom they will be used, and how it can affect their personal lives. In addition to being a legal, privacy is also an ethical obligation to establish a certain level of trust in employer and worker relationships. Concerns arise about misuse of health data for non health purposes, for example, employee surveillance or discriminatory practice (D'Arcy *et al.*, 2014). The role of RBAC has been stressed as need for data access controls in both theoretical and empirical research. These systems make sure to only allow authorised personnel to enter into sensitive health information that could instead be used illegally or

Volume 5, Issue 3, May-June-2019 | http://ijsrcseit.com

breached by anyone who wishes. It also views the roles of privacy regulations including the Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR) etc. In these regulations, standards as defined for health data security are provided and a framework within which employers must carry on their operations is drawn. Research reveals that privacy concerns in occupational health systems need to be attentively addressed to safeguard employee data, pursue ethical practises, and meet growing legal practises, inspiring further practise based research to understand better the determinants and consequences of privacy concerns in such systems.



**Figure 4** : Tactics of Identity Management (Source: Smith *et al.*, 2011)

## Methods

#### Data collection and data processing

One domain of data collection in which sensitive health information about employees is collected is in occupational health and screening systems, where health history, biometrics and health assessment results may be recorded (Smith *et al.*, 2011). The collection of this data can be made from surveys, health screening and with wearable devices and Electronic Health Records (EHRs). It is important that data privacy is kept during collection, based on strict protocol to follow of informed consent and the anonymisation of data to avoid misuse. Then, from there, the data is collected, processed to remove inconsistences, normalise values and according to all privacy regulations like HIPAA of GDPR to be usable for analysis.

#### Designing of Machine Learning Models

Occupational health and screening systems involve machine learning models that create predictive capabilities of health outcomes, dangers, or aspects of employee health data. Often, these models are based on using supervised learning techniques when historical data is used to train models to predict future health conditions (Bender and Friedman, 2018). The use of privacy preserving methods like differential privacy or federated learning may be counter used to enforce that the data is only released in such a way or if you consider the data released when training the model, you guarantee that it remains confidential while learning well. Ethical issues are issues of transparency, fairness in health related predictions, as well as avoiding algorithmic bias.

#### Implementation and Deployment

The phase, the implementation and deployment, consists in integrating the machine learning models in the operational occupational health systems. This means setting up secure data pipelines for the models, integrating models into existing health screening workflows, and integrating real time data processing with privacy regulations. They take care of the encryption of the data, the grants to be able to access the data and a continuous checking of the performances of the model to mitigate the risks of a data breach or ethical problems. We evaluate ongoing the impact of the models on employee privacy, safety, and health outcomes, making sure the models will continue to uphold ethical and legal standards.





#### Result

#### Predictive Analytics in Sales and Demand

Sales and demand forecasting using predictive analytics relies on historical sales and demand patterns, trends in the market and customer behaviour, to predict future sales and demand demand. Businesses can use machine learning algorithms, such as time series analysis, regression models and classification techniques, to find trends and forecast demand fluctuations, and to optimise inventory levels (Guo et al., 2011). How well predictive analytics work is measured by comparing the demand forecast to the real sales and improving the accuracy and the model. This also helps to see seasonal variations, demand patterns increases and decreases, as well as perform below par products, so the businesses can adjust their marketing and sale strategies as early as possible. Results improve inventory management, reduce inventory overstocking and understocking, and help with more efficient resource allocation.



Figure 6: Predictive Analytics in Sales and Demand (Source: <u>https://www.datatobiz.com/</u>) Innovation Strategies for Inventory Management and

# Replenishment

and Inventory management replenishment, innovation strategy based on optimising stocks levels and reducing operational inefficiencies through data solutions. The application of the following methods minimising waste and enhancing for the responsiveness of the supply chain includes Just in Time (JIT) inventory, automated reordering systems, and demand driven replenishment. Using technologies like Internet of Things (IoT), artificial intelligence (AI), and so on, businesses can monitor inventory time and time, and in real time, automatically re-order when inventory thresholds are reached (Katsnelson et al., 2014)

. However, these strategies are dependent on continuous analysis of data and use factors such as demand covers, lead times, and supplier's performance to enhance accuracy and reduce carrying costs. This results in faster and more economical inventory management system that adapts stock levels to real demand.

#### Redesigning the Lines of Logistics and Supply

The logistics and supply of the line requires redrawing its related lines of logistics and supply with optimization transportation routes, delivery times and warehouse systems to achieve more effective and cheaper. Employing data analytics, AI driven route optimization, and simulation techniques, companies can optimise logistics operations, reduce fuel consumption and improve delivery times (Moreira et al., 2012). This redesign course also entails the application of warehouse management systems as well as the robotic and drone in the handling as well as sorting of inventories. This results in a responsive and less expensive logistics flow, which benefits through adaptive position, reduction of operational delay risks, and increased supply chain efficiency. However, then sustainability is often incorporated into the redesigning engineering processes and sustainability pertains to the footprints of carbon and the utilisation of these green logistics solutions.

#### Discussion

Modern supply chains are the result of the combination of predictive analytics, inventory management innovation, and logistics optimization. Predictive analytics has improved the accuracy of demand forecasting and helped companies make data driven decisions that save the costs of inventory and improve service levels (Mittelstadt et al., 2016). Further, operations have been made more efficient through more innovative inventory management strategies, such as automated replenishment and real time monitoring, as well as redeigned logistics networks that result in more efficient transportation and distribution systems. But there are challenges such as data privacy, continuous model refinement that I need to do and the adaptability of new technologies in dynamic market environments. What ethical considerations are still important in these changing systems? Continuing to ensure transparency when taking these AI driven decisions and mitigating biases in demand forecasting are two vital ones.

#### **Future Directions**

AI, IoT, and machine learning are driving the landscape within supply chain management, and their future presence will undoubtedly influence the future of supply chain management itself. Depending on their maturity, these technologies will allow more sophisticated solutions for sales forecasting, inventory management and logistics leading to fully integrated, autonomous supply chains. Future research will logically concentrate on further extending the seamless integration of these technologies into end to end system; further enhancing real-time decision making and the operational efficiency. Data privacy has already become a concern and the tack should be adjusted to developing privacy preserving analytics techniques and still be able to use the predictive models (Robson et al., 2010). Also, sustainability will be a major priority for companies, and will begin to call for more environmentally friendly practises within supply chains. Such things as optimising logistics routes for lower emissions, and using bio materials in their packaging, and energy efficient warehousing solutions are examples. They will also meet broader corporate social responsibility and environmental goals, but also increase operational performance.

#### Conclusion

This concludes that maintaining employ employee health information privacy, ethically, while keeping with technological advancements pace to occupational health and screening systems is equally important. While being able to leverage some innovations (such as AI & machine learning) for more efficiency and a bit of predictive edge does mean sticking to those regulations and ethical lines. We need to continue to ensure that we maintain transparency, that we have informed consent, and that we actually have access control to sensitive health data. The security and effectiveness of these systems will need to continue to be improved while the systems will need to overcome challenges yet to

come, reflecting a need for continued research and technological refinement.

#### REFERENCES

- Fernández-Alemán, J.L., Señor, I.C., Lozoya, P.Á.O. and Toval, A., 2013. Security and privacy in electronic health records: A systematic literature review. Journal of biomedical informatics, 46(3), pp.541-562.
- [2]. Nielsen, K., Randall, R., Holten, A.L. and González, E.R., 2010. Conducting organizationallevel occupational health interventions: What works?. Work and Stress, 24(3), pp.234-259.
- [3]. D'Arcy, J., Herath, T. and Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: A coping perspective. Journal of management information systems, 31(2), pp.285-318.
- [4]. Smith, H.J., Dinev, T. and Xu, H., 2011. Information privacy research: an interdisciplinary review. MIS quarterly, pp.989-1015.
- [5]. Bender, E.M. and Friedman, B., 2018. Data statements for natural language processing: Toward mitigating system bias and enabling better science. Transactions of the Association for Computational Linguistics, 6, pp.587-604.
- [6]. Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E., 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of management information systems, 28(2), pp.203-236.
- [7]. Katsnelson, B.A., Privalova, L.I., Gurvich, V.B., Kuzmin, S.V., Kireyeva, E.P., Minigalieva, I.A., Sutunkova, M.P., Loginova, N.V., Malykh, O.L., Yarushin, S.V. and Soloboyeva, J.I., 2014. Enhancing population's resistance to toxic exposures as an auxilliary tool of decreasing environmental and occupational health risks (a self-overview). Journal of Environmental Protection, 5(14), pp.1435-1449.

- [8]. Moreira, I.C., Amaral, I., Domingues, I., Cardoso, A., Cardoso, M.J. and Cardoso, J.S., 2012. Inbreast: toward a full-field digital mammographic database. Academic radiology, 19(2), pp.236-248.
- [9]. Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S. and Floridi, L., 2016. The ethics of algorithms: Mapping the debate. Big Data and Society, 3(2), p.2053951716679679.
- [10]. Robson, M.E., Storm, C.D., Weitzel, J., Wollins, D.S. and Offit, K., 2010. American Society of Clinical Oncology policy statement update: genetic and genomic testing for cancer susceptibility. Journal of clinical oncology, 28(5), pp.893-901.