Global Trends in Science and Technology

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

Harnessing Artificial Intelligence for Cybersecurity in Healthcare and Food Processing: A Review of Emerging Trends and the Role of Generative Models like ChatGPT

Nahid Neoaz[1*]

[1]Wilmington University, USA

[1]nahidneoaz@yahoo.com

open access

Corresponding Author
Nahid Neoaz
nahidneoaz@yahoo.com

Article History:
Submitted: 09-06-2025
Accepted: 18-07-2025
Published: 24-07-2025

Keywords

Artificial Intelligence, Cybersecurity, Healthcare, Food Processing, ChatGPT, Resilience, Predictive Analytics.

ABSTRACT

Through this review we will discuss how the use of Artificial Intelligence (AI) including tools such as ChatGPT can help improve cybersecurity in both the healthcare and food processing industries. With an increase in smart technologies and digital infrastructure in these industries, cyber threats are also increasing at risk of harming patient safety, food integrity, and consumer confidence. The article looks at the roles of AI systems at detecting threats in real-time, predictive analytics, and auto-response systems, as well as real-world examples of a breach and breakthroughs. The ethics is dealt with including data privacy, bias, and transparency, as well as up-and-coming tendencies in resilient cyber-physical systems and cross-sector cooperation. The adoption of AI is presented as not only one of the defensive mechanisms, though, rather, as a strategically valuable means to construct adaptive, intelligent, and ethically responsible security systems. The article ends with a way forward towards the creation of cyber resilience in the environment where the world continues to grow digitalized and interconnected.

INTRODUCTION

The implementation of Artificial Intelligence (AI) has turned into a game changer in most economic sectors, with healthcare and food processing sectors being of particular interest. The above two areas, despite appearing to be different, are entrenched in world well-being and community security. With the continuous growth of digital transformation, the two industries are under increased pressure, especially in the area of cybersecurity [1]. AI, which undergoes adaptive learning, is not only becoming a tool but also a strategic statistical side in protecting these spheres.

The digital transformation is deep in the healthcare. The introduction of electronic health records

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

(EHRs), telemedicine, AI-aided diagnostics, robotic surgeries, and wearable health monitors have transformed the way we take care of the patient. However, the innovations also increase the area of attacks by the cybercriminals [2]. Medical data is sensitive and even more valuable and healthcare systems are prime targets of ransom ware, data breaches, and phishing attacks. In that regard, AI is used twice: obviously, to drive the technologies of healthcare but also to keep such technologies defensible, by ensuring intelligent surveillance, anticipated threats, and quick deployment of the defense [3].

At the same time, the food industry is also experiencing a digital transformation process. Food safety, supply chain transparency, and productivity are being improved with smart sensors, automation, and Internet of Things (IoT) devices, and AI-driving quality control. However, similarly to healthcare, this industry is susceptible to cyber-attacks [4]. A weak food processing system does not only threaten production but also poses threats to the health of the society due to contamination or manipulation of supply chain. AI technologies (and in particular those developed to work with anomaly detection and real-time monitoring) are also growing in use to protect food processing operations against such threats [5].

A reason as to why healthcare and food processing are related to each other is not just the value of these industries to human lives; the interdependency of these systems and being susceptible to cyber-interference are factors that relate these two areas. These two industries have now become data-centric industries and they are data-driven environments where a breach can have a knock on effect. The nexus of desperate need and digital vulnerability puts AI at a conferential position as a critical force [6]. Also, the convergence gives access to common innovations. As an example, AI algorithms that recognize anomalies in patient records can be modified so that it can recognize anomalies in food production records. To the same extent, cybersecurity measures applied to hospital networks can be used to guide how best practices can accompany food tech settings. Such a pollination between the two disciplines when aided by adaptive AI systems has the potential to bring more resilient and smart infrastructures in both areas [7].

It is also noteworthy that the transformation of these industries with the help of AI has now become a strategic decision and not merely a technological one. The security systems based on rules cannot respond to the threats as threats evolve with new complexity and magnitude. The capability of the AI technology to work based on patterns, recognizing zero-day attacks, and automating incident-responding offer an overdue advantage [8]. Other generative AI technologies such as ChatGPT, still in some nascent stages of application to the area of cybersecurity, hold promising applications in areas of training, documentation, and even in real-time support in the analysis of an incident that can be

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

used by healthcare and food processing that are on the frontline of adopting AI, especially when it comes to cybersecurity. The intersection between them is not only an indication of shared problems, but of shared opportunities as well--opportunities that, pursued with some common sense, would point the way toward a safer, smarter and more secure future not only to the United States, but also to the rest of the world [9].

CYBER SCARE IN THE HEALTHCARE AND FOOD CHAINS: A MUTE EPIDEMIC

Along with generating tremendous operational advantages, the digital transformation of the healthcare and food processing sectors led to the existence of a secret crisis: the excessive increase of cybersecurity threats. This seemingly silent epidemic would never land in the headlines on a regular day alongside other types of epidemic such as infectious diseases, or even food recalls but can just as easily cripple systems, decrease safety, and reduce trust among people [10]. These sectors are complicated, interconnected and data-dependent which has resulted in them being lucrative targets of cybercriminals, activists and even state-sponsored attackers. In the medical field, information is life-important.

Medical records, insurance information, the diagnostic imagery, prescriptions, and even genetic data now are digitalized, frequently being kept on a cloud [11]. As much as this simplifies the process of patient management and sharing information, it presents an enormous attack surface. The Ransom ware attacks on hospitals have already led to the disruption of essential care delivery, the delay of surgeries, and more tragically resulted in the death of patients. Hackers are also aware that healthcare systems are experiencing great pressure to stay in operation and will most likely pay ransoms to resume operations in the shortest time possible [12].

The IT systems within healthcare institutions are also very fragmented along with legacy software and lacking cybersecurity experts, which makes them even more vulnerable. The connection of the Internet of Medical Things (IoMT) devices, e.g., pacemakers, and insulin pumps brings even more weak points, which are often poorly secured. Hack on those systems may translate to the physical, posing a threat to lives directly. The food industry has another series of cyber risk that is equally dangerous [13]. The new potential attackers and havoc drivers arrive, as increasingly automated and connected processing facilities, supply chains, cold storage systems, and quality control are being introduced. This was the case in 2021 when the ransomware struck one of the major meat processing companies in the industry derailing their operations in several countries prompting food provision issues. It is also possible that an attack on a food supply chain at a critical point will create product shortage, price increases, and even panic by the population, or maybe the poor safety of the food product as important control systems can be compromised [14].

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

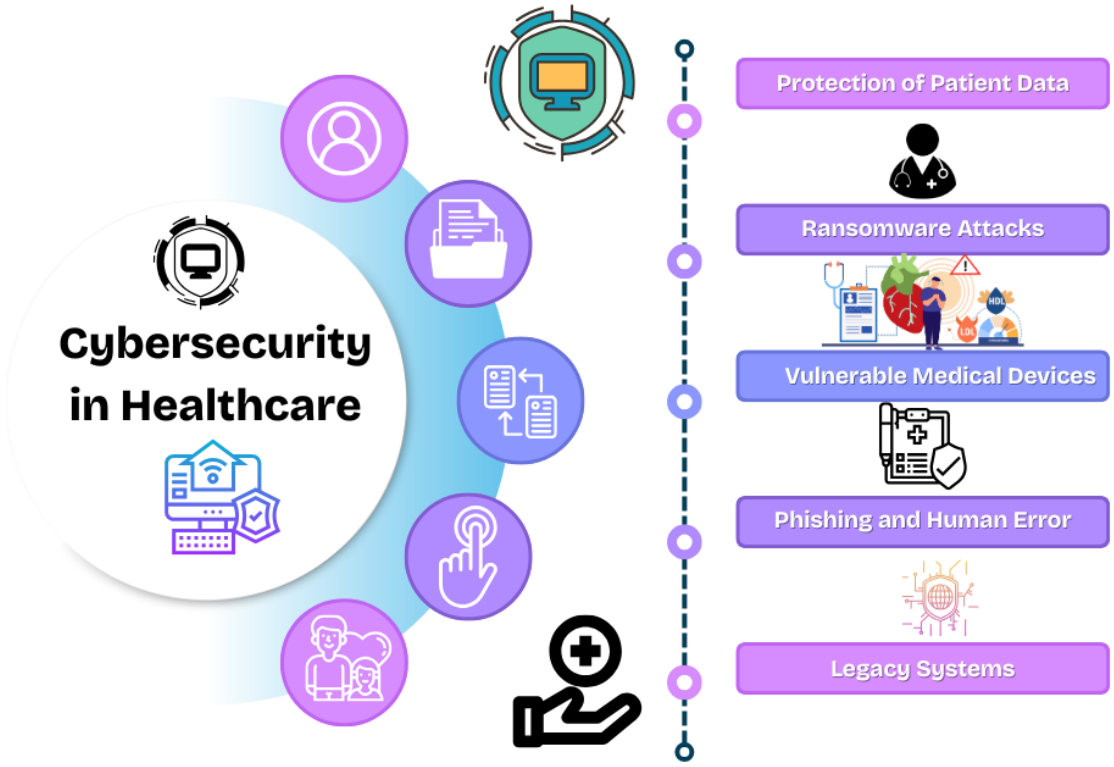

Figure: 1 showing role of cybersecurity in healthcare

The concepts illustrated in the simulation of mechanical systems, fluid dynamics, and control apparatus can be well suited into AI-powered solutions of supply chains in healthcare. As an example, simulation of the two-link planar anthropomorphic manipulator immediately reflects the accuracy expected during robotic assisted surgeries and rehabilitative devices where AI would provide precision with regard to control of its movements and ability to adapt to the individual circumstances of the patient [15]. Equally, computational fluid dynamics (mesh optimization and parameter analysis) may be applied to enhance AI models that can induce a simulation of blood flow or drugs throughout a human body, which can result in a more accurate diagnosis and treatment planning [16]. Moreover, the controlling and architectural design of the balancing mechanisms is an instance of how AI-based feedback systems can ensure balance in a life-saving setup, e.g. an autonomous patient vitals monitoring system, or a smart infusion system [17]. Collectively, all of these engineering solutions lead to the basis of AI applications, which increase the level of precision, efficiency, and safety in contemporary healthcare. Not only biologically, but digitally, the healthcare and food systems are on attack. It is no longer a matter of choice to react and to address this silent epidemic. It concerns the safety of people, healthy economy, and national security.

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

Cyber threats are evolving at a very high rate and therefore current security models are ineffective. The current attack mechanisms are faster and smarter than the static firewalls, signature based antivirus programs and rule based monitoring systems. Since the threat actors become more versatile (due to the use of automation, obfuscation techniques, and social engineering), healthcare and food processing organizations also need equally adaptable defense strategies [18]. That flexibility is provided by Artificial Intelligence (AI). AI is turning the paradigm of cybersecurity on its head by acting as an intelligent-proactive approach to security besides a reactionary shield through information gathering, pattern identification, and anomaly forecast [19].

Detection and response to threats may be considered one of the most consequential contributions of AI. In contrast to rule-based solutions that identify attacks using pre-determined packages of known malware, AI models, particularly machine learning (ML) ones, can detect traces of abnormal activity that are hard to recognize as such through predetermined signatures. As an example, within a hospital network, AI may keep track of the data access patterns and report the anomalies, including an employee, who accesses vast amounts of patient information at an unusual time of the day [20]. AI can be used to identify the anomalous behaviors of the control systems in food processing plants, which can indicate that an automation protocol was breached. Such abilities make it possible to identify them early enough, sometimes even before a major breach has taken place.

AI is also important in behavioral analytics. Learning the expected behavior of users, devices and systems means that AI will be able to spot unusual behaviors which may indicate an insider threat or than a user account has been compromised or that lateral movement has been achieved by an attacker. Behavior AI can be particularly useful in such industries as healthcare where employees need frequent access to sensitive information and systems outside of the organization and through numerous devices [21]. One planned step such as viewing patient records that are not related to the department that one works in can be flagged out and a conventional system may not detect them. Containment and remediation are faster with the use of AI in incident response. Fully automated AI is able to block infected systems, deactivate suspected accounts, or trigger processes to temporarily reverse changes during a previously learned process, often taking only a few seconds. This is an important speed in areas where any form of delay may translate to loss of operation, danger and loss of lives [22].

The phishing detection and prevention is also changing with the use of AI. Email is still one of the typical attack areas in both the medical and food industries. It is now possible to run the AI program through any emails sent-out, in order to scan for language, links and types of behavior, so that

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

messages displaying suspect actions are flagged or quarantined before they are seen by a human being. Besides, AI makes it possible to conduct constant vulnerability management. It is able to scan the software, firmware, and hardware settings of an organization through its infrastructure so as to determine the weak points, misconfigurations, and unprotected systems [23]. This vigilance has great value in fields where adherence and up-time are pertinent.

Nevertheless, there are some pitfalls to artificial intelligence-based cybersecurity. One can use false positives, algorithm bias, and a large dataset size that must be of high quality to be effective. In addition, the danger of AI vs. AI is also possible the attackers manipulate the security of AI using adversarial AI to either jump over other security or act as a poison on the training data. As such, AI needs to be coupled by human supervision, strong governance and enhancements in order to be effective [24]. The shift in the AI-driven cybersecurity field is transforming the conventional method of protection to the moving defense. This change is not only a good thing as it can be in healthcare, and the food processing industry where system integrity directly correlates with public safety. By using AI-enabled shields, these industries are not responder to mitigate threats, but predictors, to outsmart them [25].

CHATGPT AND BEYOND: GENERATIVE AI AS A CYBER ALLY

The generative AI is putting a distinctive niche into the ecosystem of cybersecurity by owning tools such as ChatGPT. Although the generative models are commonly listed as the tools of natural language processing, content creation, and customer service, today, they are considered to be strategic solutions by helping to protect digital assets, specifically in areas such as healthcare and food production, where security is paramount. In such a mode of business where uptime, precision and trust are highly crucial, conversational AI can be of significant advantage due to its adaptability and smartness. Real-time assistance and decision support are some of the most urgent areas of cybersecurity application of ChatGPT [26]. Response teams usually work with the fast-changing information, difficult logs, and documentation when faced with a security incident. ChatGPT can be an artificially intelligent helper who reads log files, proposes response protocols, and even writes incident reports on the fly. In case of a healthcare facility or a food processing plant, the availability of immediately accessible AI can help the facility drastically lower the reaction speed [27].

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

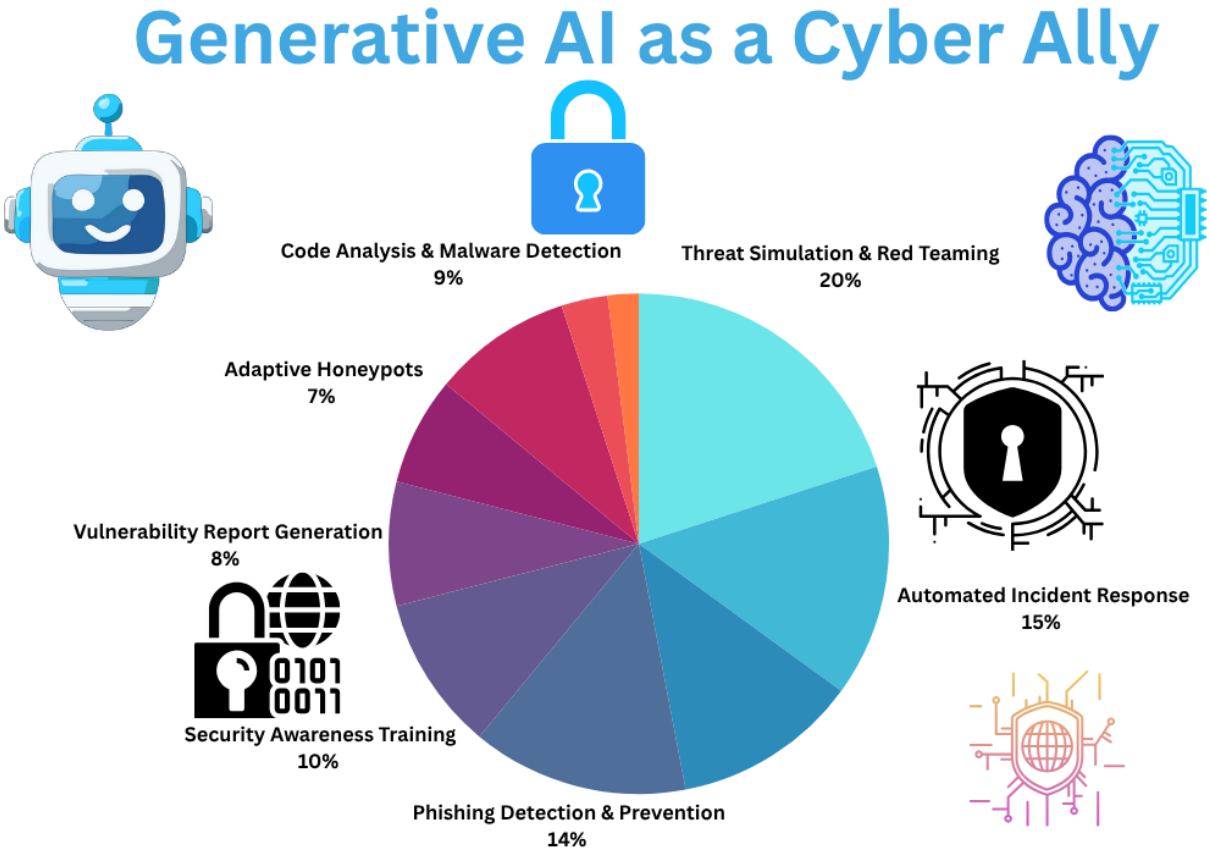

Figure: 2 showing generative AI as a cyber-Ally

There is also another important opportunity in cybersecurity education and consciousness. Most breaches originated by human mistake-getting hooked by phishing messages, improperly handling sensitive information, or picking low-quality passwords. ChatGPT may be utilized to conduct phishing training simulations, create tailored course materials and provide interactive cyber-security training to the staff. In contrast to fixed training sessions, AI-based ones have the potential to adjust to the level of knowledge of the user, keeping the level of interest and relevance at a high level [28]. Generative AI is also good at automated documentation that is very important in the highly regulated industry such as healthcare and food. By generating compliance reports, summarizing risk assessment, or creating documentation on incident response, ChatGPT can provide consistence, accuracy, and timely work.

Threat intelligence and cybersecurity research Languages such as ChatGPT can be used to scrutinize huge volumes of threat data and summarize information, and is even capable of formulating security policies in readable human language. It closes the communication gap among technical parts of cybersecurity experts and business decision-makers, helping them act quicker, with more information

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

[29]. Nevertheless, the increased potential of generative AI poses emerging security risks as well. Malicious hackers have the opportunity to use ChatGPT to develop persuasive phishing emails, social engineering scripts, or fragments of malicious codes. Such a dual-use character evinces the importance of regulated release, ethical standards, and constant monitoring of generative AI software. Nevertheless, ChatGPT and similar solutions are the future of collaboration between humans and machines when it comes to the cybersecurity field. They are swift allies, strong not only in preventing system moribundity, but in raising the people who control the systems [30].

BREACHES, BREAKTHROUGHS AND LESSONS LEARNED: CASE STUDIES

To know the real world effects of cybersecurity strategies employed in cases of healthcare and food processing we need to look at the situation through incidents both failures and success stories. Case studies help to give the vital details about how the cyber threats develop, the reaction of the organizations to them, and how much can be learnt to build better defenses in the future. The consequences of compromised systems are high in such life-essential industries because they may lead to incomplete care, poisoned food, or worst loss of lives [31]. Using several interesting examples, we learn how AI, even such a tool as ChatGPT, is starting to take a significant part in reformulating responses.

A well-known case was in 2021, when a ransom ware attack targeted Ireland national healthcare system (HSE) on the state. The hackers infiltrated through a phishing attack which allowed them to encrypt major components of the systems and compel the hospitals to book cancellations and resort to manual methods. This incident pointed out the fact that even a single mistake by a human can cause massive interruption of services [32]. Nowadays, the Irish medical staff started using AI-driven email filter, behavior pattern verification, and risk prediction within their protection measures to minimize the probability of the reoccurrence.

In the food industry, the JBS Foods cyber-attack in 2021, a ransom ware attack on the largest meat-processing firm in the world, temporarily shut down operations at both locations in the U.S. and Canada as well as in Australia. It interfered with meat markets and increased the cost of the meat to people. The food industry nurtures an interdependent system of digitization, which is revealed in the attack by the criminal organization, presumably, with the help of advanced ransom ware-as-a-service mechanisms [33]. After the breach, JBS and other food producers found themselves investing in anomaly detection systems based on AI to oversee operational technologies and industrial control systems in real-time.

On the innovation front, one of the major hospital networks in the United States recently implemented ChatGPT-powered applications to improve simulated training within its own environment and

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

optimize the creation of conformity records. Employees could train using simulated phishing threats designed and controlled by generative AI to offer them the ability to practice in a moving and changing threat landscape [34]. The outcomes were positive: the speed at which employees reacted towards real phishing attacks did improve, and there was a noticeable rise is the levels of compliance towards cybersecurity policy.

The other successful example is of a food packaging company that used AI in tracking their temperature and equipment behaviors throughout their supply chain. When the unusual spikes of data were observed and indicated that one of the refrigeration units could be tampered, the AI reported the problem to the security team to react in time before the products spoiled [35]. These incidents shed some light on one obvious conclusion active cybersecurity with the help of AI is an absolute must and not a choice. Violations persist to reveal weaknesses, but innovations are the way to go. As management uses AI systems and generative tools in real-life operations, organizations are not catching up, they evolve [36].

FOOD TO PONDER: AI FOOD SECURITY TO SMART FOOD SECURITY

Automation, data analytics, and Internet of Things (IoT) devices constitute the so-called smart food technology that is giving a major push to the global food industry. The food production, processing and distribution industries are being transformed through the use of digital tools, whether via precision agriculture to automated food processing lines and blockchain-powered supply chains. However, with innovation there is susceptibility [37]. The more systems are complex and interconnected, the more risk of cyberattacks, and it should become a threat to not only the business itself but also to the well-being of people and food safety.

The food processing plants are backed with intelligent sensors, robot arms, and industrial control systems which observe temperature, humidity, risk of contamination, and quality of products wherever they are even at a very low value. Such systems have a tendency to be connected to the cloud services or outside networks, thus presenting themselves as possible attack vectors. The hacking of such systems might entail the alteration of production parameters, food poisoning, obstruction of supply chains or even deliberate food recalls [38].

This is where AI turns out to be a life-saving cybersecurity ally. The recent developments of machine learning algorithms allow high-fidelity real-time monitoring of thousands of parameters and mark abnormalities that could represent sabotage, failure, or unauthorized intrusions. As an example, when a cooling mechanism in a meat processing plant does not act properly, say under the possible interference, AI is likely to realize it and raise signals or automatic mechanisms of shutting down, prior to the point where the food will be contaminated. What is more, AI is involved in risk

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

management in supply chains as well [39]. Modern food systems are connected with the complicated logistics and global suppliers. The risk modeling using AI will locate the areas of weakness in the chain, fraud, trace authenticity via blockchain data and provide complete chain visibility. This minimizes risks of the disruptions or tampering of data caused by cyber factors in transit.

Predictive maintenance is another field that is increasing. AI can predict when the machines or sensors at a processing plant will not work, so measures can be taken in advance, and it also blocks possible vulnerabilities to cyberattacks that could be caused by underperforming or outdated devices. Generative AIs such as ChatGPT also fit this mold. They may assist the food safety department to capture the incidents, understand the reports in natural language, create automated checklists, and even cybersecurity training of the workers in the plant, who do not typically have any technical knowledge yet are the key in keeping production secure [40].

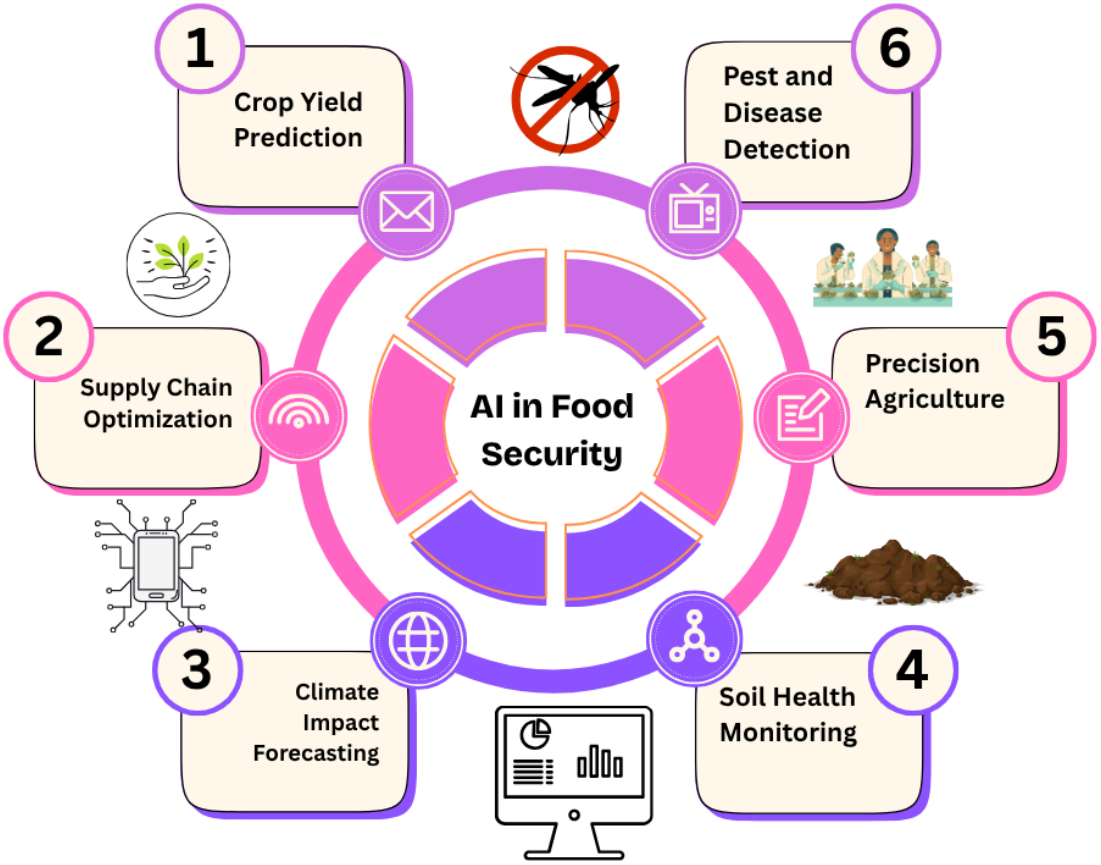

Figure: 3 showing AI role in food security

Nevertheless obstacles remain. Food businesses of small and mid-sized companies do not have the necessary resources to develop the high-tech cybersecurity infrastructures. AI should be adaptable to the environment in which it is implemented and training their workforce is essential so that they embrace it. Put it simply, the more intelligent the food tech becomes, the more intelligent the

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

protection systems need to be [41]. AI is not just another additional protection - it is gradually becoming not only a fundamental defense mechanism that makes sure that the food we consume is safe, secure and remains reliably delivered in an increasingly digital world.

THE ETHICAL EDGE: A THING AMID INNOVATION, PRIVACY AND SECURITY

With further development of artificial intelligence transforming the sphere of cybersecurity in the healthcare industry and in food processing, a vital side is likely to be ignored: ethics. Although AI helps to detect threats more quickly, make smarter automation and be predictive, its implementation provokes fundamental questions connected to privacy, bias, transparency, and accountability. Such considerations are especially delicate when it comes to the sectors involved in ensuring the health, nutrition and well-being of people. Patient information cannot be compromised in the health sector [42]. Cybersecurity/or diagnostic AI systems may request access to extensive data beyond the user interface with sensitive personal health information (PHI). Unless dealt with accordingly, this data can be open to exposure, misuse and even transfer without the correct authority. Re-identification attacks are applicable even to the anonymized data sets. The task of striking a balance between the necessity of AI models to study real-life data and the duty to secure individual privacy is rather fragile yet one that cannot be neglected [43].

In food processing, the data is often less personally sensitive, but issues of ethical concern concern the transparency of the supply chain, the ownership of data and the automation-induced effects on labor. The suppliers, partners, or employees might be the ones that the AI system monitoring production line or a supply chain can store information on. Who is the owner of that data? What is its application? These are important questions in the era of decision-making AI. Algorithmic bias is one more important problem [44]. When healthcare or food safety AI models are trained on either skewed or incomplete data, the models can yield a biased output. This may be the situation in healthcare where predisposed people may cover and others may be over-marked as risks. There may also be an issue of market fairness as biased AI models in the food industry would tend to fall against smaller-scale producers when measuring quality or conformity needs [45].

Ethical concern such as transparency is also of concern. AIs, particularly those using the deep learning models, may perform as a black box more often than not: they may generate an output that is not well-explained. Decisions made with the help of an AI recommendation should be explainable and traceable in crucial areas such as healthcare. Both patients and professionals have a right to know why a system indicated a possible violation or identified one or another condition [46]. In addition, there exist fears of misinformation, excessive use, and information accuracy as generative AI apps, such as ChatGPT, will become part of a workflow. As an illustration, even planned incident response

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

plans or security documents created with the use of ChatGPT require human supervision to proof their factual correctness, contextual appropriacy, and ethical soundness [47].

HIPAA regulatory framework currently provides some degree of guidance in the sphere of healthcare, and many other food safety standards of compliance (ex. FSMA or GFSI) follow suit, however, they are still lagging behind the blistering pace of AI technologies. The ethical edge of AI in healthcare and food cybersecurity is not a constraint but a guide. IT organizations have to pass what the law mandates and start to position ethics-by-design into the development and deployment of AI systems, and that is privacy, fairness, and accountability. Innovation has to be consonant with humanity [48]. Privacy has to be respected by security. The advancements should not compromise with trust. In this Janus-like balancing act, we must be clever and thoughtful so as to design AI that transcends smart to be right [49].

FUTURE TRENDS AND STRATEGIC ROADMAP TO TOWARD RESILIENCE

The mere fact that the digital infrastructure of healthcare and food processing industries is continuing to grow implies that one should no longer ask whether these two sectors would ever be exposed to cyber threats, but only how frequently and effectively would these particular industries survive and overcome them. Greater defenses are not the only way forward in cybersecurity in these key sectors, but resilience: the capacity to expect, absorb, adjust and recover to the attack must be generated in the cyber world. This evolution is focused on Artificial Intelligence (AI) particularly in its combination with strategic foresight and ethical governance [50].

Among the most vivid tendencies, one can embrace the transition between reactive and predictive security. Machine learning and AI models are to be improved that will help predict the threats early enough by relying on past data, behavior pattern detection and real-time surveillance. In the case of healthcare, this may imply that the presence of ransom ware or an insider threat can be detected a few days, or even weeks in advance of its emergence [51]. In food processing it may mean detecting anomalies in supply chain behavior or production patterns that may be indicative of tampering or sabotage.

Autonomous response systems will also emerge in the future, which includes the systems of AI agents that can isolate breached systems, re-route traffic in networks, fix vulnerabilities, and even interact with the human teams during the incidents. Combined with faster response time and the possibility of what is known as self-healing networks, the importance of these systems increase when it comes to risks to human life or even the safety of populations. The other emerging area is cyber physical security [52]. With increasing inclusion of smart devices, IoT, and industrial control systems in food manufacturing and medical care, it will be crucial to secure physical assets by relying on cyber

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

intelligence. AI is going to watch and protect everything, including robotic surgical systems, hospital HVAC systems, and cold storage and packaging machines [53].

The tools of generative AI such as ChatGPT will increasingly be used to automate compliance reporting, to code complex cybersecurity procedures in human-readable forms, to conduct multilingual education in operations around the world, and even in communicating an incident to stakeholders or the population. The more advanced the models get, the more they will be used in operations, policy development, and even in ethical audit. At the same time, cross-sector collaboration is to be given more attention [54]. Healthcare and food cybersecurity cannot be in a silo. Cooperating between the level of governments, tech companies, regulators, and on the frontline organizations is necessary to stop and remove the threats by communicating threat intelligence, create open standards together, and finance innovation. Sharing of threats might become commonplace- attack signature and anomaly patterns being shared in real time across geography and industries [55].

CONCLUSION

Living in the times of ever-increasing digitalization, artificial intelligence (AI) and cybersecurity transcend into a new era of defending such vulnerable fields of life as healthcare and food processing against the more and more hack-savvy cyber-crimes. The success of human health, quality of life and social stability largely depends on these industries, and in that regard, cybercriminals have them in their sights, proving that the market of intelligent, adaptive, and resilient security products is more necessary than ever.

The need to have an interconnected medical device, electronic medical records, and telemedicine sites has advanced to the point where medical institutions depend on them. At the same time, food production systems are becoming smarter and are connected into ecosystems and are supported by IoT, robotics and data-driven logistics. Such digital connectivity has resulted in tremendous operational gains - and way bigger attack surfaces as well. Such complex systems are targeted by cybercriminals with their goal to steal sensitive data, bring operations to a halt, or sever supply chains. It is against this background that the concept of AI only serves as a tool, but a shaking force. AI is paving a new mode of thinking on the cyber protection. Machine learning models will allow detecting anomalies in real-time and even predicting potential attacks based on previous approaches that are not otherwise possible with traditional security systems. In healthcare, AI may be used to secure the patient records, track networks in hospitals and prevent any threats that may cause harm before it can result. When used in food processing, it locks lines of production, alerts about inconsistency in the supply chain data, and makes sure that automation is not a source of vulnerability.

Generative artificial intelligence, such as ChatGPT, is auxiliary and is growing in strategies. These

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

models are useful during training, incident response, documentation of policy, and even prepares phishing to enhance awareness of employees. Yet they come with a dual-use potential, its power can be bent to create persuasive attacks, so their application should come with caution. Ethical use, human control, and ethics are, therefore, necessary. The scenarios that are examined in the real world, like the situation in the Irish healthcare where the ransom ware attacks and the JBS Foods that got hacked, demonstrate that there is much to lose and many ill repercussions to being unprepared. They also show us a way forward: an organization that incorporates AI in order to create flexible security systems and that uses lessons learned about past breaches and uses them to constantly improve. Proactive and AI-based resilience is not a trend but a reality.

Moral issues cannot be left on the wayside in this process. The most relevant element of the AI deployment is the concern of protecting privacy, preventing bias, being transparent, and upholding the human agency. Ethical AI is not an option in the industries where choices may alter lives or compromise the safety of the population. Going forward, the way to resilience is through strategic planning and cultural change. It demands more than a commitment to smart technology, though--it demands an investment in people and partnerships, in preparation. Organizations have to integrate AI in their cybersecurity roadmaps, but not as a solution that works right now, but an evolving environment- able to learn, evolve, and react to new threats.

Teamwork is also going to be an important factor. The pillars of resilient cybersecurity infrastructure will be cross sector collaboration, government reinforcement, and unified threat intelligence and industry standards. Artificial intelligence can contribute to making this a possibility, transforming disjointed defenses to network-based, smart protection. Finally, the application of AI to the sphere of cybersecurity is not only a technological breakthrough. It is a pointer to a new era where systems are resilient, i.e. not only secure, but resistant, recoverable and prosperous in the face of tribulation. This evolution is not only about data or device security in healthcare or food processing, but also about human health safety, guarantee of food security, and maintenance of the trust of the people. We can construct a cybersecurity system as flexible and intelligent as the malware that challenges it, a system that might not only be able to protect our systems, but our common future by adopting AI with moral clarity, strategic purpose, and working together.

REFERENCES

[1]. Khan M, Shiwlani A, Qayyum MU, Sherani AM, Hussain HK. AI-powered healthcare revolution: an extensive examination of innovative methods in cancer treatment. BULLET: Jurnal Multidisiplin Ilmu. 2024 Feb 28;3(1):87-98.

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

[2]. Kakadiaris IA, Vrigkas M, Yen AA, Kuznetsova T, Budof M, Naghavi M. Machine learning outperforms ACC/AHA CVD risk calculator in MESA. J Am Heart Assoc. 2018; 7:e009476.

[3]. Liu T, Fan W, Wu C. A hybrid machine learning approach to cerebral stroke prediction based on imbalanced medical dataset. Artif Intell Med. 2019; 101:101723–101723.

[4]. Cutillo CM, Sharma KR, Foschini L, Kundu S, Mackintosh M, Mandl KD. Machine intelligence in healthcare—perspectives on trustworthiness, explainability, usability, and transparency. NPJ Digit Med. 2020; 3:1–5.

[5]. Tonekaboni S, Joshi S, McCradden MD, Goldenberg A. What clinicians want: contextualizing explainable machine learning for clinical end use. ArXiv190505134 Cs Stat. 2019. http://arxiv.org/abs/1905.05134.

[6]. Accessed 3 Sept 2019. 24. Institute of Medicine (US) Committee on Quality of Health Care in America. Crossing the quality chasm: a new health system for the 21st century. Washington, DC: National Academies Press (US); 2001. http:// www.ncbi.nlm.nih.gov/books/NBK222274/. Accessed 21 May 2020.

[7]. Shiwlani A, Khan M, Sherani AM, Qayyum MU, Hussain HK. Revolutionizing healthcare: The impact of artificial intelligence on patient care, diagnosis, and treatment. JURIHUM: Jurnal Inovasi dan Humaniora. 2024 Feb 28;1(5):779-90.

[8]. Barry MJ, Edgman-Levitan S. Shared decision making—the pinnacle patient-centered care. N Engl J Med. 2012; 366:780–1

[9]. Kunneman M, Montori VM, Castaneda-Guarderas A, Hess EP. What is shared decision making? (and What it is not). Acad Emerg Med. 2016; 23:1320–4.

[10]. Valli LN. Predictive Analytics Applications for Risk Mitigation across Industries; A review. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(4):542-53.

[11]. Malik FS, Sahibzada S, Nasir S, Lodhi SK. Machine Learning-Enhanced Turbulence Prediction and Flow Optimization for Advanced Aerodynamic Design in High-Speed Regimes. European Journal of Science, Innovation and Technology. 2024;4(6):39-46.

[12]. Kumar S, Shiwlani A, Hasan SU, Kumar S, Shamsi F, Hasan S. Artificial Intelligence in Organ Transplantation: A Systematic Review of Current Advances, Challenges, and Future Directions.

[13]. Asif SM. Simulation of A Two Link Planar Anthropomorphic Manipulator. BULLET: Jurnal Multidisiplin Ilmu.; 1(03):539-52.

[14]. Asif SM. Analysis of Key Parameters and Mesh Optimization in Computational Fluid Dynamics Using Open FOAM. BULLET: Jurnal Multidisiplin Ilmu.; 1(2):592455.

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

[15]. Asif SM. Design and Control of A Ball and Beam Balancing Mechanism Using MATLAB/Simulink. Global Journal of Multidisciplinary Sciences and Arts.; 1(2):1-34.

[16]. Nizamullah FN, Zeb S, Abbasi N, Qayyum MU, Fahad M. AI in Healthcare: Breaking New Ground in the Management and Treatment of Cancer. Asian Journal of Engineering, Social and Health. 2024 Oct 18;3(10):2325-43.

[17]. Zeb S, Lodhi SK. AI and Cybersecurity in Smart Manufacturing: Protecting Industrial Systems. American Journal of Artificial Intelligence and Computing. 2025 Apr 7;1(1):1-23.

[18]. Javeedullah M. Integrating Health Informatics Into Modern Healthcare Systems: A Comprehensive Review. Global Journal of Universal Studies.;2(1):1-21.

[19]. Shehzad K, Munir A, Ali U. AI-Powered Food Contaminant Detection: A Review of Machine Learning Approaches. Global Journal of Computer Sciences and Artificial Intelligence.;1(2):1-22.

[20]. Samad A. Internet of things integrated with blockchain and artificial intelligence in healthcare system. Research Journal of Computer Systems and Engineering. 2022 Oct 15;3(1):01-6.

[21]. Zeb S, Lodhi SK. AI for predictive maintenance: Reducing downtime and enhancing efficiency. Enrichment: Journal of Multidisciplinary Research and Development. 2025 May 13;3(1):135-50.

[22]. Choi JE, Qiao Y, Kryczek I, Yu J, Gurkan J, Bao Y, Gondal M, Tien JC, Maj T, Yazdani S, Parolia A. PIKfyve, expressed by CD11c-positive cells, controls tumor immunity. Nature Communications. 2024 Jun 28;15(1):5487.

[23]. Nizamullah F, Fahad M, Abbasi N, Qayyum MU, Zeb S. Ethical and legal challenges in AI-driven healthcare: patient privacy, data security, legal framework, and compliance. Int. J. Innov. Res. Sci. Eng. Technol. 2024;13:15216-23.

[24]. Javeedullah M. Security and Privacy in Health Informatics: Safeguarding Patient Data in A Digital World. AlgoVista: Journal of AI and Computer Science.;2(3):52-68.

[25]. Zeb S, Nizamullah FN, Abbasi N, Qayyum MU. Transforming Healthcare: Artificial Intelligence's Place in Contemporary Medicine. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(4):592385.

[26]. Valli LN, Sujatha N. Predictive Modeling and Decision-Making in Data Science: A Comparative Study. In2024 5th International Conference on Recent Trends in Computer Science and Technology (ICRTCST) 2024 Apr 9 (pp. 603-608). IEEE.

[27]. Lodhi SK. Synaptic Harmonies: Applying Graph Coloring Algorithms to Mental Health AI Systems. Global Journal of Emerging AI and Computing. 2025 Jan 26;1(1):83-91.

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

[28]. Nasir S, Zainab H, Hussain HK. Artificial-Intelligence Aerodynamics for Efficient Energy Systems: The Focus on Wind Turbines. BULLET: Jurnal Multidisiplin Ilmu. 2024;3(5):648-59.

[29]. Qayyum MU, Sherani AM, Khan M, Shiwlani A, Hussain HK. Using AI in Healthcare to Manage Vaccines Effectively. JURIHUM: Jurnal Inovasi dan Humaniora. 2024 May 27;1(6):841-54.

[30]. Shiwlani A, Kumar S, Qureshi HA. Leveraging Generative AI for Precision Medicine: Interpreting Immune Biomarker Data from EHRs in Autoimmune and Infectious Diseases. Annals of Human and Social Sciences. 2025 Feb 20;6(1):244-60.

[31]. Gondal MN, Chaudhary SU. Navigating multi-scale cancer systems biology towards model-driven clinical oncology and its applications in personalized therapeutics. Frontiers in Oncology. 2021 Nov 24; 11:712505.

[32]. Abbasi N, Nizamullah FN, Zeb S, Fardous MD. Generative AI in healthcare: revolutionizing disease diagnosis, expanding treatment options, and enhancing patient care. J Knowl Learn Sci Technol 3 (3), 127–138. ISSN: 2959-6386 [Internet]. 2024

[33]. Lodhi SK, Zeb S. Ai-Driven Robotics and Automation: The Evolution of Human-Machine Collaboration. Journal of World Science. 2025 May 13;4(4):422-37.

[34]. Shehzad K, Munir A, Ali U. Modern Trends in Food Production: the Role of AI in Smart Food Factories. Global Journal of Emerging AI and Computing.;1(2):1-30.

[35]. Javeedullah M. Using Health Informatics to Streamline Healthcare Operations. American Journal of Artificial Intelligence and Computing. 2025 Apr 7;1(1):24-44.

[36]. Shehzad K, Ali U, Munir A. Computer Vision for Food Quality Assessment: Advances and Challenges. Available at SSRN 5196776. 2025.

[37]. Abbasi N, Nizamullah FN, Zeb S, Fahad M, Qayyum MU. Machine learning models for predicting susceptibility to infectious diseases based on microbiome profiles. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). 2024 Aug 25; 3(4):35-47.

[38]. Shehzad K, Ali U, Munir A. Role of AI in Food Production and Preservation. Global Insights in Artificial Intelligence and Computing. 2025 Feb 19;1(2):1-7.

[39]. Samek W, Montavon G, Vedaldi A, Hansen LK, Müller K-R, editors. Explainable AI: interpreting, explaining and visualizing deep learning. Berlin: Springer; 2019. https://doi.org/10.1007/978-3-030-28954-6

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

[40]. Esteva A, Robicquet A, Ramsundar B, Kuleshov V, DePristo M, Chou K, et al. A guide to deep learning in healthcare. Nat Med. 2019; 25:24–9. 8.

[41]. Islam SR, Eberle W, Ghafoor SK. Towards quantifcation of explainability in explainable artifcial intelligence methods. ArXiv191110104 Cs Q-Fin. 2019. http://arxiv.org/abs/1911.10104.

[42]. Samek W, Montavon G, Lapuschkin S, Anders CJ, Müller K-R. Toward interpretable machine learning: transparent deep neural networks and beyond. ArXiv200307631 Cs Stat. 2020. http://arxiv.org/abs/2003.07631.

[43]. Accessed 2 Oct 2020. 10. Lapuschkin S, Wäldchen S, Binder A, Montavon G, Samek W, Müller K-R. Unmasking Clever Hans predictors and assessing what machines really learn. Nat Commun. 2019; 10:1096.

[44]. Abbasi N, Nizamullah FN, Zeb S. AI in healthcare: integrating advanced technologies with traditional practices for enhanced patient care. BULLET: Jurnal Multidisiplin Ilmu. 2023 Jun 13;2(3):546-6.

[45]. George AS. AI-enabled intelligent manufacturing: A path to increased productivity, quality, and insights. Partners Universal Innovative Research Publication. 2024 Aug 25;2(4):50-63.

[46]. Javeedullah M. Bridging Technology and Care: The Role of Health Informatics in Modern Healthcare. American Journal of Artificial Intelligence and Computing. 2025 Jun 30;1(2):1-22.

[47]. Abbasi N, Nizamullah FN, Zeb S. Ai in healthcare: Using cutting-edge technologies to revolutionize vaccine development and distribution. JURIHUM: Jurnal Inovasi dan Humaniora. 2023 Jun 14;1(1):17-29.

[48]. Javeedullah M. Role of Health Informatics in Public Health Surveillance and Response. American Journal of Artificial Intelligence and Computing. 2025 Apr 21;1(1):70-86.

[49]. Gondal MN, Shah SU, Chinnaiyan AM, Cieslik M. A systematic overview of single-cell transcriptomics databases, their use cases, and limitations. Frontiers in Bioinformatics. 2024 Jul 8;4:1417428.

[50]. Zech JR, Badgeley MA, Liu M, Costa AB, Titano JJ, Oermann EK. Variable generalization performance of a deep learning model to detect pneumonia in chest radiographs: a cross-sectional study. PLOS Med. 2018; 15:e1002683.

[51]. Olsen HP, Slosser JL, Hildebrandt TT, Wiesener C. What's in the box? The legal requirement of explainability in computationally aided decisionmaking in public administration. SSRN

ISSN : 3079-5761
Volume 1, Number 3, 2025
https://doi.org/10.70445/gtst.1.3.2025.144-162

Scholarly Paper. Rochester: Social Science Research Network; 2019. https://doi.org/10.2139/ssrn.3402974

[52]. Schönberger D. Artifcial intelligence in healthcare: a critical analysis of the legal and ethical implications. Int J Law Inf Technol. 2019; 27:171–203.

[53]. Cohen IG. Informed consent and medical artifcial intelligence: what to tell the patient? SSRN Scholarly Paper. Rochester, NY: Social Science Research Network; 2020. https://doi.org/10.2139/ssrn.3529576.

[54]. Beaudouin V, Bloch I, Bounie D, Clémençon S, d'Alché-Buc F, Eagan J, et al. Identifying the "right" level of explanation in a given situation. SSRN Electron J. 2020. https://doi.org/10.2139/ssrn.3604924.

[55]. Weng SF, Reps J, Kai J, Garibaldi JM, Qureshi N. Can machine-learning improve cardiovascular risk prediction using routine clinical data? PLoS ONE. 2017; 12:e0174944.