Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

Information Security and Legal Ethics of Artificial Intelligence Medical Devices

Hongrui Zhao, Gengqi Yang*
School of Humanities, Social Science & Law, Harbin Institute of Technology, Harbin, Heilongjiang, China
*Corresponding Author.

Abstract:

Due to the impact of the COVID-19 pandemic, global economic growth has slowed down and competition has intensified, and digital and intelligent transformation of enterprises has become an inevitable trend. In addition, with the continuous promotion of new infrastructure policies, the potential application scenarios of artificial intelligence are expanding, and the medical applications enabled by artificial intelligence are transitioning from the early surfacing stage to the in-depth exploration stage. Under the industry consensus of "patient-centered and practical to meet the needs of doctors' clinical work", the potential dangers of information security are gradually highlighted, posing an unprecedented challenge to the security of information under AI medical. Due to the special nature of the medical device industry and the lag of the industry's supporting legal system, AI in the medical device field lacks a perfect information security regulatory system, and this status quo will inevitably bring great uncertainty and instability to the long-term development of AI in the medical device field. This paper discusses the classification of information security issues of AI at home and abroad, and further discusses the information security problems faced by AI in the field of medical devices by studying the specific classification of AI in the field of medical devices according to different needs and puts forward countermeasures and suggestions to cope with them.

Keywords*: Artificial intelligence, Medical devices, Information security.*

I. INTRODUCTION

Artificial intelligence medical devices are the specific applications of artificial intelligence technology in the field of medical devices, which as an emerging medical device in many areas to achieve breakthroughs. In addition to conventional medical devices, medical software and information systems are also included in the category of medical devices. The International Medical Device Regulator (IMDRF) defines software as a medical device, i.e., stand-alone software whose purpose is to be used for one or more "medical purposes" and which, in fulfilling those "medical purposes," is "medical purposes" without being part of the hardware of a medical device [1].

The State Council in 2017 issued the "New Generation of Artificial Intelligence Development Plan" clearly put forward the development direction of the intelligent medical part, and in 2018 the National Health Care Commission issued the "National Health Care Big Data Standards, Security, and Services

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

Management Measures (for Trial Implementation)" (National Health Planning Development [2018] No. 23) to clearly specify the standards and security principles for the use of medical big data, and in July 2019, the Artificial Intelligence Medical device innovation cooperation platform was established, aiming to actively address the new risks and challenges brought by the rapid development of AI to regulation and industry; coordinate forces, coordinate the role of all parties in data management, standard development, clinical evaluation, testing and inspection, and strive to establish a scientific evaluation system for AI medical devices in China; encourage innovation and accelerate the transformation and application of AI scientific and technological achievements in the field of medical devices.

Medical workers use medical devices, medical software and information systems that are empowered by artificial intelligence[2] , so while we actively encourage the development of artificially intelligent medical devices, we need to recognize the problems and implications of artificially intelligent medical devices as a new generation of technology products in terms of information security and other aspects.

II. THE CURRENT SITUATION OF INFORMATION SECURITY ISSUES OF ARTIFICIAL INTELLIGENCE AT HOME AND ABROAD

The term "artificial intelligence" was first introduced by John McCarthy at the Dartmouth Conference in 1956, and since then there have been different views on the definition of artificial intelligence. In Artificial Intelligence - A Modern Approach, AI is defined in four categories: systems that think like humans, systems that act like humans, systems that think rationally, and systems that act rationally. Encyclopedia Britannica qualifies AI as the ability of a digital computer, or a robot controlled by a digital computer to perform a number of tasks that only an intelligent organism has. The 2018 Chinese White Paper on Standardization of Artificial Intelligence defines AI as the use of a digital computer or a machine controlled by a digital computer to simulate, extend, and expand human intelligence, perceive the environment, acquire knowledge, and use the knowledge to obtain optimal results theories, methods, technologies, and application systems.

It is certain that with the breakthrough and development of AI in key technologies such as machine learning, knowledge mapping, natural language processing, computer recognition, human-computer interaction and biometric identification, AI has become the core driver of a new round of industrial change. However, because the AI technology itself and its applications in various fields are still in the development stage, in the face of the current world information security situation, huge data information and diverse means of cybercrime, it is no longer possible to solve the information security problem in the AI era by simply relying on traditional methods, and domestic and foreign political circles and scholars have emphasized the importance of information security in the AI era, and ensuring information security is the Ensuring information security is an important prerequisite for the sustainable and healthy development of AI technology.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

2.1 Foreign artificial intelligence information security status

In October 2016, the U.S. released the National Artificial Intelligence Strategic Plan for Research and Development, which identifies seven major government programs focused on funding research in the field of artificial intelligence, including "ensuring the safety and security of AI systems. The U.S. then reported on the socioeconomic impact of AI in the strategy document "Ready for the Future of Artificial Intelligence," and the two reports together proposed an "AI Open Data" initiative. In December of the same year, the White House Office of Science and Technology Policy documented the U.S. approach to artificial intelligence in the Trump years in "Science and Technology Matters - Memories of the First Year of the Trump Administration" and released the report "Artificial Intelligence, Automation, and the Economy." In February 2019, U.S. President Donald Trump money number "Artificial Intelligence Initiative" development plan, further instructions on data openness. In June 2019, the U.S. released a new version of the National Artificial Intelligence R&D and Development Strategic Plan, which requires all agency heads to focus on data security, privacy, and confidentiality protection.

In 2016, the U.K. government released the report "Opportunities and Impact of Artificial Intelligence on Future Decision Making," which focused on the impact of AI on personal privacy, and in the same year, the House of Commons Science and Technology Committee released the report "Robotics and Artificial Intelligence," which raised the challenges of AI in information security. 2017, AI was included in the government report "An Industrial Approach: Building a Britain for the Future. In 2017, AI was included in the government report "Industrial Approach: Building Britain for the Future".

The UK and the US specifically focus on five AI information security issues in the aforementioned government reports and strategic plans: 1. Transparency and trustworthiness, both countries regard transparency as the primary indicator of AI security and controllability, but with current technology, there is no effective way to track the AI decision-making process; verifiability and confirmability, secure AI systems require new methods of assessment, stand-short methods and maintenance methods; ethics and privacy, in response to people's sensitivity to data-intensive AI algorithms going wrong and misuse, the privacy protection and data rights issues brought about by big data are magnified, and the technical deterioration can also lead to other social problems; responsibility model, mainly refers to the designers and deployers of AI systems should take and in responsibility for the results of AI system behavior; security protection and long-term optimization. Emphasis on traditional cybersecurity in the AI environment may bring new challenges and threats such as widespread shall-be cyber-attacks [3].

The EU has issued policies related to artificial intelligence since 2014.In 2014, the report "European Robotics Strategy 2014-2020" and the "Horizon 2020 Strategy - Multi-year Development Strategy Map for Robotics" were published. In May 2016, the Legal Affairs Committee of the EU Parliament published the "Draft Recommendation to the EU Committee on Civil Law Rules for Robotics". In October 2016 the EU Civil Law Rules on Robotics was published in October 2016, actively focusing on the legal liability of AI. 2018 EU countries signed a declaration on AI collaboration, and the EU Political Strategy Centre published "The Age of Artificial Intelligence: establishing a human-centered European strategy" in March

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

of the same year, raising the issue of data shortage and data bias in the development of AI in Europe, and expanding the program of data sources for AI systems to ensure that the General In April 2018, the European Commission released the draft EU Artificial Intelligence, proposing to build a code of ethics for AI and an appropriate legal framework to provide a trustworthy and accountable environment for AI. December 2019 saw the release of the Artificial Intelligence Coordination Plan to implement the EU Artificial Intelligence Strategy.

Japan announced the New Strategy for Robotics in January 2015 and warped the importance of information collection and processing as well as personal information handling in the Artificial Intelligence Technology Strategy report released in March 2017.the fifth edition of the Next Generation Artificial Intelligence and Robotics Core Technology Development Plan was released in April 2018, proposing to build data-driven and knowledge fusion and to study the balance between data security and privacy protection.

Germany was the first to propose the national strategy of "Industry 4.0" in 2011, released the "New High-Tech Strategy" in 2014, enacted the country's first autonomous driving law in May 2017, and released the document "Highlights of the Federal Government's Artificial Intelligence Strategy" in July 2018, requiring the federal government to increase funding for AI-related fields.

France launched the French Robotics Development Plan in 2013, formulated the National Artificial Intelligence Strategy in 2017 with specific recommendations for policies to develop AI, and released the French AI Development Strategy in March 2018, in which the report states that the development of French AI will focus particularly on the four areas of health, transportation, environment, and defense and security, proposing the implementation of an open data policy that Focus on areas such as open public data, data exchange platforms, and health data centers.

The Indian government think tank released its National AI Strategy in June 2018, focusing applications on five major areas of healthcare, agriculture, education, smart cities, and infrastructure and smart transportation, and specifically instilling the areas of military security and ethical privacy, with specific strategic plans proposed in the report for data bias, data protection, and privacy protection mentions.

South Korea announced the "BRAIN" plan for artificial intelligence in March 2016 and identified nine national strategic projects including artificial intelligence in August of the same year.

Russia does not yet have a government-level strategy document in place, but the country places great emphasis on breakthroughs in AI from academic and industrial sources, with a particular bias toward the development and autonomy of AI technologies for military and defense applications.

Overall, it seems that the importance of information security is emphasized in AI strategy documents at the government level around the world, but there are huge differences in the level of AI technology, data resources and laws and regulations in each country, and because of this, strengthening information security

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

will play an important role in the development of AI around the world.

2.2 China's artificial intelligence information security status

In 2016, the Development and Reform Commission released the "Internet + Artificial Intelligence Three-Year Action Implementation Plan", which proposed to accelerate the sea-linked training resource base and public platform of basic resource services for multiple types of data.

In July 2017, the State Council issued the "Development Plan for a New Generation of Artificial Intelligence", clearly proposing that while vigorously developing AI, it is important to pay great attention to the security risk challenges that may be posed, strengthen forward-looking prevention and constraint guidance, minimize risks, and ensure safe, reliable, and controlled development of AI; accelerate the in-depth application of advanced AI technologies in the field of cybersecurity; focus on Artificial intelligence data security, emphasizing data security, privacy protection, and strengthening data management risk prevention.

In December 2017, the Ministry of Industry and Information Technology released the Three-Year Action Plan for Promoting the Development of a New Generation of Artificial Intelligence Industry (2018-2020), which further proposed plans for data opening.

In January 2018, the China Institute of Electronic Technology Standardization released a white paper on the standardization of artificial intelligence, pointing out that since the recent development of artificial intelligence is based on the application of information technology wisdom to a large amount of data, there should be a clear and operational definition of privacy issues involving personal information, and the access to and knowledge of personal data in the context of artificial intelligence should likewise be redefined.

In 2019, the "AI Data Security White Paper" released by the China Academy of Information and Communication Research clearly puts forward data security as the key to AI security and proposes an AI data security system with three dimensions, including risk, application, and governance.

Comprehensive view, China's artificial intelligence in the field of information security or there is security risk prevention technology research and means of construction relatively lagging the problem [4].

III. CLASSIFICATION OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN THE FIELD OF MEDICAL DEVICES

In the face of the current situation of high cost, low efficiency and uneven material level of traditional medical care, patient demand presents chronic diseases as the mainstream, the number of aging more than the number of diseases, the rise of national health awareness and other aspects of change, the concept of artificial intelligence & medical was born. And with the breakthroughs in machine learning, semiconductor

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

technology and other hardware and software, artificial intelligence technology in the medical device field has achieved a blowout development results [5-10].

Medical devices are legally defined as instruments, equipment, apparatus, in vitro diagnostic reagents and calibrators, materials and other similar or related items used directly or indirectly on the human body, including the required computer software. According to the "Medical Device Regulations" Article 4, the state of medical devices in accordance with the degree of risk management: the first category is a low level of risk, the implementation of conventional management can ensure the safety and effectiveness of medical devices; the second category is a medium risk, the need for strict control of management to ensure its safety and effectiveness of medical devices; the third category is a higher risk, the need to take special measures to strictly control the management to In 2017, the "Medical Device Classification Catalog" was released, containing 22 sub-categories, 206 product categories and 1,157 product categories.

Artificial intelligence medical devices have not yet entered the medical device classification catalog in China. Therefore, if we want to discuss the classification of AI applications in medical devices, we should consider their specific needs in medical scenarios. In this paper, we will classify AI medical devices according to three aspects: pre-hospital prediction, in-hospital treatment, and post-hospital rehabilitation.

3.1 Pre-hospital projections

The main purpose of pre-hospital prediction is to enhance individual health risk prediction, improve the overall health of the population, and reduce the probability of major diseases. Wearable medical devices, for example, are portable, wearable smart devices that continuously monitor the monitored person's own signs over a long period of time to keep track of their body functions. For example, in 2016, the U.S. Food and Drug Administration (FAD) approved a new artificial insulin that incorporates wearable devices for real-time monitoring, which can monitor the blood glucose level of the monitored person in real time, analyze the real-time data through artificial intelligence software, and inject insulin into the monitored person when needed to ensure the stability of the patient's blood glucose level [11].

3.2 In-hospital treatment

In-hospital treatment is mainly used to assist in the diagnosis of diseases, improving the efficiency of doctors' diagnosis and reducing the rate of misdiagnosis; in participating in the treatment process to assist in treatment, achieving a more stable and accurate treatment plan and easily realizing real-time monitoring, intelligent surgical robots are the effective combination of image processing assisted diagnosis systems, robots, and surgeons. For example, researchers at Google examined the fundus retinal photographs of 11,000 patients and came up with a predictive value of up to 99.8%, proving that artificial intelligence in this technology can already surpass the diagnostic accuracy and efficiency of ophthalmologists in aiding diagnosis.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

3.3 Post-hospital rehabilitation

Under the traditional model, post-hospital rehabilitation is difficult to achieve due to the difficulty for doctors to take care of post-hospital follow-up and the lack of rehabilitators. Artificial intelligence technology, on the other hand, can be combined with hardware and software to achieve post-hospital rehabilitation for patients.

In general, the application of artificial intelligence in the field of medical devices mainly exists in two categories: software, the combination of medical images and artificial intelligence technology, such as the current application of the more common "intelligent reading" type of AI medical software [12]; hardware, the use of artificial intelligence technology to enable hardware[13-15].

IV. INFORMATION SECURITY ISSUES OF ARTIFICIAL INTELLIGENCE IN MEDICAL DEVICE FIELD

Information security includes confidentiality, availability, integrity, and controllability of information [16]. The application of artificial intelligence in healthcare is everywhere related to data, and the risk of data is reflected in all aspects of information security risk, such as personal data leakage, privacy protection, network security, etc.

4.1 Personal data and privacy protection

The principle of "respecting privacy" is clearly stated in the "Principles of New Generation Artificial Intelligence Governance - Developing Responsible Artificial Intelligence" released by the National Professional Committee on New Generation Artificial Intelligence Governance in 2019. Artificial intelligence in medical devices should ensure the safety and integrity of patient privacy and prevent the leakage of personal data and privacy. In fact, artificial intelligence in the field of medical devices is supported by big data, requiring many training samples to achieve high quality and efficient data collection, most of the training samples in this field come from various types of data from hospital patients, such information will certainly involve the privacy of patients [17].

However, there are no clear standards on such information security issues in China, and it mainly relies on the consciousness of companies and users. The main data privacy protection guidelines available are the European General Data Protection Regulation (GDPR), which came into effect in 2018 in the European Union, and the Health Insurance Portability and Accountability Act (HIPAA), published by the U.S. Congress in 1996 [18] . The European General Data Protection Regulation clearly defines personal data, medical health-related data [19]. The Health Insurance Portability and Accountability Act both protects health information that is private to individuals and ensures that researchers have ongoing access to the medical information necessary to conduct research.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

4.2 Network viruses and system vulnerabilities

Although the application of artificial intelligence in the field of medical devices usually exists in a closed network environment, it can still be technically invaded and penetrated by hackers through firewalls, and the result of the execution of these attackers' corrupted medical devices will seriously affect their security. The medical devices infected with computer viruses, after spreading and replicating through the network, there will be a batch of the same type of medical devices infected, which in turn will affect the health of tens of thousands of people.

On the other hand, the system itself may exist involving lack of money or system vulnerability. Medical device software under artificial intelligence is becoming increasingly complex and diverse, and unlike software quality testing in other industries, software quality failures in medical device scenarios will directly affect the safety of medical devices and even the lives and health of patients.

4.3 The lag of laws and regulations

Laws and regulations are an important means of information security regulation, according to China's laws, the Food and Drug Administration is responsible for the supervision and management of medical devices, and the public security part is responsible for public information network security supervision. However, the proposed information security laws for artificial intelligence medical devices will require a longer time cost and will inevitably lag the current technological development. China currently for artificial intelligence data security laws and regulations, there is a lack of systematic documents, the relevant legal provisions, although mentioned in the "Network Security Law", "Electronic Commerce Law" and other laws, but for the current field of new technology development, there is a lack of perfect legal support.

V. CONCLUSIONS

As mentioned earlier, the development of artificial intelligence in the medical device field is coming on strong and poses a potential challenge to information security. In today's increasingly important information security issues, the potential dangers of technology applications in information security after being empowered by AI pose an unprecedented challenge to information security. Due to the special nature of the medical device industry and the lagging legal system, AI in the medical device field lacks a comprehensive information security regulatory system, and this status quo will inevitably bring great uncertainty and instability to the long-term development of AI in the medical device field. In the face of AI-enabled medical devices, the information security regulatory concept must be actively addressed by the home team, clearly recognizing the risks, and proceeding simultaneously from the technical and non-technical levels to seize the strategic research opportunities.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

5.1 Improve information security supervision risk regulation measures and strengthen personal data and privacy protection

In accordance with relevant national laws and regulations, relying on industry organizations or third-party organizations, the implementation of supervision and inspection of information security issues in the field of artificial intelligence medical devices to achieve early detection and early treatment, and reduce the harm caused by such problems to patients and society. Rely on the existing technical means to strengthen the information security governance capabilities of artificial intelligence in the field of medical devices.

5.2 Strengthen the research and development of information security technology of artificial intelligence

Encourage the academic community to carry out research on information security risk incentives and defense mechanisms of artificial intelligence in the field of medical devices, encourage enterprises to improve technical design and enhance technical measures, take advantage of their own advantages, and actively carry out research and development of related products.

5.3 Establish a sound safety standard system

Under the AI security standards, combine information security standards and medical device security standards to develop data security standards for AI in the field of medical devices to promote the work. Organize domestic enterprises, scientific research units and other multifaceted forces to promote the introduction of China's AI data security standards in combination with the international standardization system in related fields. Through the United Nations, G20 and other international platforms, actively participate in international dialogue and cooperation, and participate in the development of international artificial intelligence information security norms.

5.4 Promote relevant legislation

Promote the introduction of relevant legislation on artificial intelligence and information security, improve relevant departmental regulations on artificial intelligence and information security, strengthen law enforcement, and promote the effective implementation of relevant laws and regulations at the national and local levels. Clarify the legal principles of information security in the field of medical devices, establish the data rights and information security responsibilities of different subjects, and prevent problems such as excessive data collection, waste of resources and information leakage.

REFERENCES

[1] Editorial Board of China Food and Drug Administration. Medical device software based on artificial intelligence and machine learning technology. China Food and Drug Administration. 2019.6(185):59-61.

Forest Chemicals Review
www.forestchemicalsreview.com
ISSN: 1520-0191
July-August 2022 Page No. 236-245
Article History: Received: 30 March 2022, Revised: 8 April 2022, Accepted: 15 April 2022, Publication: 30 April 2022

[2] Tang QIAO Hong, Wang H, Ren H-P. Ethical issues in artificial intelligence medical devices. China Pharmaceutical Affairs. 2019(9):1004-1008.
[3] Wang Yipeng. Information security on AI development in the UK and US national strategies for AI. Net Matters Focus. 2018 (05):67-69.
[4] China Academy of Information and Communication Research. Artificial Intelligence Data Security White Paper (2019).
[5] Lecun Y, Bengio Y, Hinton G. Deep learning. Nature, 2015, 436.
[6] Lindholm E, Nickolls J, Oberman S. NVIDIA Tesla: a unified graphics and computing architecture. IEEE Micro, 2008, 28(2):39-55.
[7] Becker AS, Marcon M, Ghafoor S. Deep learning in mammography: diagnostic accuracy of a multipurpose image analysis software in the detection of breast cancer. Invest Radiol, 2017, 52(7):434.
[8] Esteva A, Kuprel B, Novoa RA. Dermatologist-level classification of skin cancer with deep neural networks. Nature, 2017, 542:115-118.
[9] Lee H, Tajmir S, Lee J. Fully automated deep learning system for bone age assessment. J Digit Imaging, 2017, 30: 427.
[10] Setio AAA, Traverso A, de Bel T. Validation, comparison, and combination of algorithms for automatic detection of pulmonary nodules in computed tomography images: the LUNA16 challenge. Med Image Anal, 2017, 42: 1-13.
[11] Chen JW. Deep integration of artificial intelligence and healthcare. China Health. 2017, (9):102- 103.
[12] Jin Lei, Xie L. An overview of network security. Computer Engineering and Design. 2003, 24 (2):19-22.
[13] FDA. Cardinal Health Alaris Infusion Pump Module (formerly Medley Pump Module), Model 8100 Class 1 Recall. (2007-10-29). http://www.fda.gov/Medical Devices/Safety/ListofRecalls/ucm062366.htm.
[14] China.com, South Korea explodes medical equipment due to connection network may also chant hacking. (2013-08-07). http://www.china.com.cn/news/world/2013-08/07/cotent_29648627.htm.
[15] Zhang Q., Liu S. L., Yan Y. Analysis of medical device products recalled by the U.S. FDA in 2005-2006. China Journal of Medical Devices. 2011, 35 (4):280-283.
[16] Zhang Chenguang, Liu Yan, Xu Wei. Research and countermeasures on information security of intelligent medical devices. China Pharmacovigilance. 2015 (06):51-53.
[17] Tang QIAO-HONG, Wang H, Ren H-P. Ethical issues in artificially intelligent medical devices. China Pharmaceutical Affairs. 2019(9): 1004-1008.
[18] Liu, L. Y., Gao, S. Z., Shang, J. et al. Biomedical research provisions in the U.S. Health Insurance Portability and Accountability Act and their implications. Chinese medical ethics. 2016, 29(6):1011-1014.
[19] Wang Hao-Chen. Impact of the EU General Data Protection Regulation on the development of artificial intelligence and its inspiration. China Economic and Trade Journal: Theory Edition, 2018, 900 (17):22-24.