HISAR SCHOOL
JUNIOR MODEL UNITED NATIONS 2025

Protecting Democracy in an Age of Severe Political Polarization and Extremism by promoting constructive discourse

SA3: Health Committee

Impeding the issue of cyber attacks on patient and individual data within healthcare systems

BERKE BALLIEL

RESEARCH REPORT

Forum: Health Committee (SA3)

Issue: Impeding the issue of cyber attacks on patient and individual data within healthcare systems.

Student Officer: Berke Ballıel - President Chair

Introduction

The issue of cyber attacks on patient and individual data in healthcare systems has become a big problem globally because of the growing number of digitalized records used in hospitals and reliance on interconnected systems to easily reach a patient's important information in an emergency case. Even though this system has made it easy for medical personnel to understand the patient's illness and help in time, it has also made individuals' records more vulnerable to cyber threats. These attacks aim to take over the personal and medical information of the patients and directly breach personal privacy.

Definition of Key Terms

Electronic Health Records (EHRs): EHR is the systemized collection of patient data, electronically stored in a digital format.

Cybercrime: Cybercrime is a criminal activity that either targets or uses a computer, a computer network, or a networked device. (Kaspersky)

Identity Theft: One's personal or financial information being used without their permission. (usa.gov)

Cyberattack: A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. (Cisco)

Remote care: Remote care is a medical service that allows providers to have access to real-time health evaluations of patients outside the care of a hospital by using remotely connected monitoring and medical devices. (virtusa.com)

General Overview

The issue of cyber attacks on healthcare systems has become a growing global problem, dating back to the late 1990s and early 2000s as more and more hospitals and healthcare centers started to rely on computer and digital systems to keep track of patient records. However, this issue has become more significant during the 2010s, as considerably more healthcare systems have adopted electronic health

records (EHRs), begun using connected devices and systems, and cybercrimes/criminals have become more common in the world with the rise of electronic systems like computers and mobile phones.

Healthcare systems are appealing targets for cybercriminals due to the high value of information they hold. Patient and individual data include medical histories, insurance information, social security numbers, and financial records, all of which can be sold on illegal marketplaces such as the black market or be used for identity theft and fraud. Furthermore, cyber-attacks on healthcare systems can involve ransomware, where hackers can lock all interconnected systems, demanding payment for the hospital to regain access to the system. This hack has become more and more common in recent years, with big attacks disrupting hospital and clinic duties, delaying treatments, and putting patient safety at risk.

Poor cybersecurity training for medical staff makes medical organizations open to common tactics such as phishing, where attackers trick employees into revealing sensitive information or providing access to systems. Many institutions also have financial problems resulting in not being able to fund for better cybersecurity structure or reach out to experts to protect their systems.

The issue of cyber attacks on patient and individual data is not limited to a single region or a country but is a global problem. Cyber attacks on healthcare systems have been reported by both developed and developing nations. In developed countries, the large-scale usage of digital health technologies has made them open to cyber threats whereas underdeveloped and developing countries suffer from not having well-structured digital health systems.

The COVID-19 pandemic revealed the seriousness of cyber threats in healthcare, as hackers utilized problematic remote care systems and the fast adoption of them. During the pandemic hospitals and other research centers have become targets more usual than ever.

Governments, healthcare institutions, and technology companies have responded by taking precautions to strengthen data protection. Laws like the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) establish standards in this area but their effect depends on effective enforcement. International cooperation between Member States is important to catch cyber criminals effectively as they most often operate in various countries.

Major Parties Involved and Their Views

United States Department of Health and Human Services (HHS)

The HHS administers healthcare systems in the United States of America (USA) and implements laws like HIPAA to protect patient data. It advocates increased regulations on cybersecurity and spreads awareness about cyber threats. The HHS also provides guidelines to healthcare organizations.

European Union (EU)

The EU implements regulations like GDPR and the NIS2 Directive whilst calling for more reports on rules and more responsibility for data controllers and processors.

World Health Organization (WHO)

The WHO promotes global health security and guides healthcare organizations to protect their systems from cyber-attacks. The party also highlights the attacks' effect on disrupting important services and creating health risks. The WHO supports international collaboration to improve cybersecurity.

International Criminal Police Organization (INTERPOL)

The INTERPOL makes an effort to fight cyber criminals all across the world, including healthcare-related attacks. The party sees healthcare as an important sector under threat and calls for international collaboration.

Timeline of Events

21 August, 1996	*The Health Insurance Portability and Accountability Act (HIPAA) was signed into U.S. law, introducing guidelines for securing healthcare data.*
17 February, 2009	*The Health Information Technology for Economic and Clinical Health Act (HITECH) is signed in the U.S., promoting the adoption of electronic health records (EHRs) while raising awareness about data security.*
4 February, 2015	*Anthem Inc. announced a breach that exposed the personal data of 78.8 million individuals, making it one of the largest healthcare data breaches.*
12 May, 2017	*The WannaCry ransomware attack disrupted the UK's National Health Service (NHS), paralyzing hospitals and delaying patient care globally.*
1 January, 2025	*The European Union (EU) began enforcing the NIS2 Directive, mandating healthcare organizations to adopt strict cybersecurity measures and report breaches within 24 hours.*

Treaties and Events

The Health Information Technology for Economic and Clinical Health Act (HITECH)

This treaty has been signed in the USA and its main aim is to promote the adoption of electronic health records for all healthcare institutions while raising awareness about data security.

The Health Insurance Portability and Accountability Act (HIPAA)

This treaty is one of the first treaties to determine the criteria and the guidelines to be used while storing data related to healthcare. It was signed in the USA.

The General Data Protection Regulation (GDPR)

By holding organizations accountable for the way they use personal data, GDPR increases individuals' rights to privacy and reassures the customer. It is enforced by the EU.

Evaluation of Previous Attempts to Resolve the Issue

The HIPAA was established to set national standards in the USA for protecting data and EHRs. It has failed because HIPAA's security measures were not designed to protect the complex nature of cybersecurity. Furthermore, the HITECH Act promoted the adoption of EHRs for healthcare organizations and digitized records. Even though EHR adoption increased, this adoption was made fast, therefore opening many new cyber threats. Lastly, the GDPR enforcement was the EU's set of data protection requirements and penalties for breaches. It failed due to its unrealistic requirements that were difficult to implement.

Possible Solutions

Cybersecurity regulations can be strengthened to a certain degree. Keeping in mind high standards would tie the hands of small healthcare organizations and the opposite would make the perfect target for cybercriminals. In addition, the appropriate standards may be internationally recognized to ensure international collaboration. Lastly, with enough funding, investments in cybersecurity programs in healthcare systems and training for experts may be provided to build complex structures for cybersecurity.

Additional Resources

HHS Cyber Gateway - This platform has enough cybersecurity information from US agencies.

Cybersecurity Resouces for HIPAA-Regulated Entities - This document has helpful tools for the agenda.

Healthcare Cybersecurity: Tips for Securing Private Health Data - This article has the best tools for healthcare organizations to protect sensitive health information.

Bibliography

"Cybersecurity in Healthcare." HealthITSecurity, 2023, www.healthitsecurity.com/news/cybersecurity-in-healthcare

"Healthcare Cybersecurity: Understanding the Growing Threat." American Medical Association, 2023, www.ama-assn.org/delivering-care/public-health/healthcare-cybersecurity-understanding-growing-threat

Health Insurance Portability and Accountability Act of 1996 (HIPAA). U.S. Department of Health and Human Services, 1996, www.hhs.gov/hipaa/for-professionals/index.html

General Data Protection Regulation (GDPR). European Commission, 2018, ec.europa.eu/info/law/law-topic/data-protection_en